# Test of Vandiver's conjecture with Gauss sums Heuristics 

Georges Gras

## To cite this version:

Georges Gras. Test of Vandiver's conjecture with Gauss sums - Heuristics. 2018. hal-01856083v4

## HAL Id: hal-01856083 <br> https://hal.science/hal-01856083v4

Preprint submitted on 25 Jun 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# 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), Thaine (1995-1999) and Anglès-Nuccio (2010). This conjecture is required in many subjects and we shall give such examples of relevant references. In this paper, we recall our interpretation of Vandiver's conjecture in terms of minus part of the torsion of the Galois group of the maximal abelian $p$-ramified pro- $p$-extension of the $p$ th cyclotomic field (1984). Then we provide a specific use of Gauss sums of characters of order $p$ of $\mathbb{F}_{\ell}^{\times}$and prove new criteria for Vandiver's conjecture to hold (Theorem 1.2 (a) using both the sets of exponents of $p$-irregularity and of $p$-primarity of suitable twists of the Gauss sums, and Theorem 1.2 (b) which does not need the knowledge of Bernoulli numbers or cyclotomic units). We propose in §5.2 new heuristics showing that any counterexample to the conjecture leads to excessive constraints modulo $p$ on the above twists as $\ell$ varies and suggests analytical approaches to evidence. We perform numerical experiments to strengthen our arguments in direction of the very probable truth of Vandiver's conjecture. All the calculations are given with their PARI/GP programs.


## Contents

1. Introduction 1
2. Pseudo-units - Notion of $p$-primarity 4
3. Abelian $p$-ramification 5
4. Twists of Gauss sums associated to primes $\ell \equiv 1(\bmod p) \quad 8$
5. Heuristics - Probability of a counterexample 19
6. Conclusion 28

References 29

## 1. Introduction

Let $K=\mathbb{Q}\left(\mu_{p}\right)$ be the field of $p$ th roots of unity for a given prime $p>2$ and let $K_{+}$be its maximal real subfield. Put $G:=\operatorname{Gal}(K / \mathbb{Q})$.
We denote by $C l$ and $C l_{+}$the $p$-class groups of $K$ and $K_{+}$, then by $C_{-}$the relative $p$-class group, so that $\mathrm{Cl}=\mathrm{Cl}_{+} \oplus \mathrm{Cl}_{-}$.
Let $E$ and $E_{+}$be the groups of units of $K$ and $K_{+}$; then $E=E_{+} \oplus \mu_{p}$ (Kummer).
The conjecture of Vandiver (or Kummer-Vandiver) asserts that $\mathcal{C} \ell_{+}$is trivial. This statement is equivalent to say that the group of real cyclotomic units of $K$ is of prime to $p$ index in $E_{+}$ [52, Theorem 8.14]. One may refer to numerical tables using this property in [4, 9] (verifying the conjecture up to $2 \cdot 10^{9}$ ), and to more general results in [50, 51] where some relations

[^0]with Gauss and Jacobi sums are used to express the order of the isotypic components of $\mathrm{Cl}_{+}$ (e.g., [50, Theorem 4]).

Many heuristics are proposed about this conjecture; see Washington's book [52, § 8.3, Corollary 8.19] for some history, criteria, and for probabilistic arguments, then [38] assuming Greenberg's conjecture [22] for $K_{+}$.
We have also given a probabilistic study in [15, II.5.4.9.2]. All these heuristics lead to the fact that the number of primes $p$ less than $x$, giving a counterexample, can be of the form $O(1) \cdot \log (\log (x))$.
These reasonings, giving the possible existence of infinitely many counterexamples to Vandiver's conjecture, are based on standard probabilities associated with the Borel-Cantelli heuristic, but many recent $p$-adic heuristics and conjectures (on class groups and units) may contradict such unfounded approaches.
In this paper, we shall work in another direction, in the framework of "abelian $p$-ramification", using Gauss sums together with the "Main Theorem on abelian fields" restricted to $\mathrm{Cl}_{-}$, and giving the order of its isotypic components by means of generalized Bernoulli numbers (this aspect is related by Ribet in [40, 41] and we shall call it "Main Theorem" for short).
Such a link of Vandiver's conjecture with Gauss sums and abelian p-ramification has been given first by Iwasawa [28], then by Anglès-Nuccio [1], and encountered by many authors in various directions (Iwasawa's theory, Galois cohomology, Fermat curves, Galois representations,...), then often assuming Vandiver's conjecture (e.g., [8, 23, 24, 26, 27, 31, 44, 45, 46, 47, 53, 54]).
This link does exist also in the context of the classical conjecture of Greenberg [22] considered as a generalization of Vandiver's conjecture (e.g., [35], [16]). We propose, in Section 3.1, to explain the links with $p$-ramification and prove again the reflection theorem (Theorem 3.1 and Corollary 3.2).
Then we shall interpret a counterexample to Vandiver's conjecture in terms of non-trivial " $p$-primary pseudo-units" stemming from Gauss sums:

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

for $\psi$ of order $p, \xi_{\ell}$ of prime order $\ell \equiv 1(\bmod p)$. Indeed, if $\# \mathcal{C} \ell_{+} \equiv 0(\bmod p)$, there exists a class $\gamma=\boldsymbol{d}(\mathfrak{A}) \in \mathcal{C} \ell_{-}$, 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 a cyclic unramified extension $L_{+} / K_{+}$of degree $p$ predicted by class field theory); the reciprocal being obvious.
Since $\alpha$ can be obtained explicitely by means of twists (giving products of Jacobi sums) of the above Gauss sums:

$$
\begin{equation*}
\mathrm{g}_{c}(\ell)=\tau(\psi)^{c-\sigma_{c}} \in K, \tag{1}
\end{equation*}
$$

with Artin automorphisms $\sigma_{c}$ attached to a primitive root $c$ modulo $p$, this will yield the main test verifying the validity of the conjecture at $p$; this result is the object of the Theorem 4.7, Corollary 4.8 and Theorem 4.9, that we can summarize, in the Theorem 1.2 below, after the reminder of some notations and classical definitions.

Definition 1.1. (i) Let $\zeta_{p}$ be a primitive $p$ th root of unity. We denote by $\omega$ the Teichmüller character of $G$ (the $p$-adic character with values in $\mu_{p-1}\left(\mathbb{Q}_{p}\right)$ such that $\zeta_{p}^{s}=\zeta_{p}^{\omega(s)}$ for all $s \in G)$.
The irreducible $p$-adic characters of $G$ are the $\theta=\omega^{m}, 1 \leq m \leq p-1$.
(ii) Let $e_{\theta}:=\frac{1}{p-1} \sum_{s \in G} \theta\left(s^{-1}\right) s$ be the associated idempotents in $\mathbb{Z}_{p}[G]$.
(iii) Let $\mathrm{g}_{c}(\ell)_{\theta}$ denotes the $\theta$-component of the twist $\mathrm{g}_{c}(\ell)$ defined by (1), as representative in $K^{\times}$of the class of ${\overline{\mathrm{g}_{c}(\ell)}}^{e_{\theta}} \in K^{\times} / K^{\times p}$.

Theorem 1.2 (Main theorem). For a prime $\ell \equiv 1(\bmod p)$, let $\mathscr{E}_{\ell}(p)$ be the set of exponents of p-primarity of $\ell$ (even integers $n \in[2, p-3]$, such that $\mathrm{g}_{c}(\ell)_{\omega^{p-n}} \equiv 1(\bmod p)$ ). Then let $\mathscr{E}_{0}(p)$ be the set of exponents of $p$-irregularity of $K$ (even integers $n \in[2, p-3]$, such that $p$ divides the nth Bernoulli number $B_{n}$ ).
(a) Vandiver's conjecture holds for $K$ if and only if there exists $\ell \equiv 1(\bmod p)$ such that $\mathscr{E}_{\ell}(p) \cap \mathscr{E}_{0}(p)=\emptyset$.
(b) Vandiver's conjecture holds for $K$ if and only if there exist $N \geq 1$ primes $\ell_{i} \equiv 1$ $(\bmod p)$ such that $\bigcap_{i=1}^{N} \mathscr{E}_{\ell_{i}}(p)=\emptyset$.

Test (b) is numerically very frequent for $N=1$ or $N$ very small, and does not need the knowledge of Bernoulli's numbers; in fact, it does not need to know if $p$ is irregular or not (see Theorem 4.9).
We show that some assumption of independence, of the congruential properties $(\bmod p)$ of these twists, as $\ell$ varies, is an obstruction to any counterexample to Vandiver's conjecture.
This method is different from that needed to prove that some cyclotomic unit is not a global $p$ th power, which does not give obvious probabilistic approach (nevertheless, see $\S 5.2 .4$ for some complements).
Finally, we propose, in $\S \S 5.2,5.3$, new heuristics (to our knowledge) and give substantial numerical experiments confirming them.

Definition 1.3. (i) We denote by $\mathscr{X}_{+}$the set of even characters $\theta \neq 1$ (i.e., $\theta=\omega^{m}$, $m \in[2, p-3]$ even), and by $\mathscr{X}_{-}$the set of odd characters distinct from $\omega$ (i.e., $\theta=\omega^{m}$, $m \in[3, p-2]$ odd).
If $\theta=\omega^{m}$, we put $\theta^{*}:=\omega \theta^{-1}=\omega^{p-m}$. This defines an involution on the group of characters which applies $\mathscr{X}_{+}$onto $\mathscr{X}_{+}^{*}=\mathscr{X}_{-}$.
(ii) For a finitely generated $\mathbb{Z}_{p}[G]$-module $M$, we put $M_{\theta}:=M^{e_{\theta}}$. The operation of the complex conjugation $s_{-1} \in G$ gives rise to the obvious definition of the components $M_{+}$and $M_{-}$such that $M=M_{+} \oplus M_{-}$.
(iii) We denote by $\operatorname{rk}_{p}(A):=\operatorname{dim}_{\mathbb{F}_{p}}\left(A / A^{p}\right)$ the $p$-rank of any abelian group $A$.
(iv) For $\alpha \in K^{\times}$, prime to $p$, considered modulo $K^{\times p}$, we denote by $\alpha_{\theta}$ a representative in $K^{\times}$of the class $\bar{\alpha}^{e_{\theta}} \in K^{\times} / K^{\times p}$ (e.g., $\alpha_{\theta}=\alpha^{e_{\theta}^{\prime}}$ where $e_{\theta}^{\prime} \in \mathbb{Z}[G]$ approximates $e_{\theta} \bmod p$ ).
(v) Let $I$ be the group of prime to $p$ ideals of $K$. For any $\mathfrak{A} \in I$ such that $c(\mathfrak{A}) \in \mathcal{C l}$, there exists an approximation $e_{\theta}^{\prime} \in \mathbb{Z}[G]$ of $e_{\theta}$ modulo a sufficient high power of $p$ such that $\mathfrak{A}_{\theta}:=\mathfrak{A}^{e_{\theta}^{\prime}}$ is defined up to a principal ideal of the form $\left(x^{p}\right), x \in K^{\times}$.
(vi) We say that $\mathfrak{A} \in I$ is $p$-principal if it is principal in $I \otimes \mathbb{Z}_{p}$; thus $\mathfrak{A}=(\alpha)$, with $\alpha \in K^{\times} \otimes \mathbb{Z}_{p}$, defined up to the product by $\varepsilon \in E \otimes \mathbb{Z}_{p}{ }^{1}$
(vii) For $\chi=: \omega^{n} \in \mathscr{X}_{+}$, let $B_{1,\left(\chi^{*}\right)^{-1}}=B_{1, \omega^{n-1}}:=\frac{1}{p} \sum_{a=1}^{p-1}\left(\chi^{*}\right)^{-1}\left(s_{a}\right) a$ be the generalized Bernoulli number of character $\left(\chi^{*}\right)^{-1}$ (where $s_{a} \in G$ is the Artin automorphism attached to $a$; it is the restriction of the Artin automorphism $\sigma_{a}$ defined above in larger extensions).

[^1]The Bernoulli number $B_{1, \omega^{n-1}}$ is an element of $\mathbb{Z}_{p}$ congruent modulo $p$ to $\frac{B_{n}}{n}$, where $B_{n}$ is the $n$th ordinary Bernoulli number; see [52, Proposition 4.1, Corollary 5.15].
(viii) We say that a finitely generated $\mathbb{Z}_{p}[G]$-module $M$ is monogenous if it is generated, over $\mathbb{Z}_{p}[G]$, by a single element; this is equivalent to $\operatorname{rk}_{p}\left(M_{\theta}\right) \leq 1$ for all irreducible $p$-adic character $\theta$ of $G$.

The index of $p$-irregularity $i(p)$ is the number of even $n \in[2, p-3]$ such that $B_{n} \equiv 0$ $(\bmod p)$; thus $i(p)=\# \mathcal{E}_{0}(p)$. See [52, §5.3 \& Exercise 6.6] giving statistics and the heuristic $i(p)=O\left(\frac{\log (p)}{\log (\log (p))}\right)$.
For a general history of Bernoulli-Kummer-Herbrand-Ribet, then Mazur-Wiles-Thaine-Kolyvagin-Rubin-Greither works on cyclotomy see [13, 41, 52]; in this context, if for $\theta \in \mathscr{X}_{-}$, $B_{1, \theta^{-1}}$ is of $p$-valuation $e$, we shall have (Main Theorem):

$$
\# C C_{\theta}=\left|B_{1, \theta^{-1}}\right|_{p}^{-1}=p^{e}
$$

## 2. Pseudo-units - Notion of $\boldsymbol{p}$-primarity

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

Remark 2.2. (i) Let $A$ be the group of pseudo-units of $K$. If $\alpha \in A$, there exists an ideal $\mathfrak{a}$ such that $(\alpha)=\mathfrak{a}^{p}$; then if we associate with $\alpha K^{\times p}$ the class of $\mathfrak{a}$, we obtain the exact sequence, where ${ }_{p} \mathcal{C l}:=\left\{\gamma \in \mathcal{C l}, \quad \gamma^{p}=1\right\}$ :

$$
1 \longrightarrow E / E^{p} \longrightarrow A K^{\times p} / K^{\times p} \longrightarrow{ }_{p} \mathrm{Cl} \longrightarrow 1,
$$

giving $\operatorname{dim}_{\mathbb{F}_{p}}\left(A K^{\times p} / K^{\times p}\right)=\frac{p-1}{2}+\mathrm{rk}_{p}(\mathcal{C l})$. Thus the computation of $\operatorname{dim}_{\mathbb{F}_{p}}\left(\left(A K^{\times p} / K^{\times p}\right)_{\theta}\right)$ is immediate from the value of $\mathrm{rk}_{p}\left(\mathcal{C l}_{\theta}\right)$ and $\operatorname{dim}_{\mathbb{F}_{p}}\left(\left(E / E^{p}\right)_{\theta}\right)=1$ (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 $\alpha \in K^{\times}$( $\alpha$ prime to $p$ but not necessarily a pseudo-unit) is " $\alpha$ congruent to a $p$ th power modulo $\mathfrak{p}^{p}=(p) \mathfrak{p}$ " (e.g., [15, Ch. I, §6, (b), Theorem 6.3]). Since in any case (replacing $\alpha$ by $\left.\alpha^{p-1}\right)$ we can assume $\alpha \equiv 1(\bmod \mathfrak{p})$, the above condition is then equivalent to $\alpha \equiv 1\left(\bmod \mathfrak{p}^{p}\right)$ (indeed, for any $x \equiv 1(\bmod \mathfrak{p})$ we get $\left.x^{p} \equiv 1\left(\bmod \mathfrak{p}^{p}\right)\right)$.

For the pseudo-units of $K$, the $p$-primarity may be characterized 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 pth power at $\mathfrak{p}$.

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

When $\alpha$ is not necessarily a pseudo-unit, we have a similar result provided we only look at the $p$-primarity of $\alpha_{\theta}$ for $\theta \neq 1, \omega$ :

Proposition 2.4. Let $\alpha \equiv 1(\bmod \mathfrak{p})$. Let $m \in[2, p-2]$ and let $\alpha_{\theta}$ for $\theta=\omega^{m}$. Then $\alpha_{\theta} \equiv 1\left(\bmod \mathfrak{p}^{m}\right)$; moreover $\alpha_{\theta}$ is p-primary if and only if $\alpha_{\theta} \equiv 1(\bmod p)$, in which case one gets $\alpha_{\theta} \equiv 1\left(\bmod \mathfrak{p}^{m+p-1}=(p) \mathfrak{p}^{m}\right)$.

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

Put $\alpha_{\theta}=1+\varpi^{k} u$, where $u$ is a unit of $\mathbb{Z}_{p}[\varpi]$ and $k \geq 1$; let $u_{0} \in \mathbb{Z} \backslash p \mathbb{Z}$ be such that $u \equiv u_{0}$ $(\bmod \varpi)$ giving $\alpha_{\theta} \equiv 1+\varpi^{k} u_{0}\left(\bmod \varpi^{k+1}\right)$. Since $\alpha_{\theta}^{s}=\alpha_{\theta}^{\theta(s)}$ in $K^{\times} \otimes \mathbb{Z}_{p}$, we get, for all $s \in G:$

$$
1+s\left(\varpi^{k}\right) u_{0}=1+\omega^{k}(s) \varpi^{k} u_{0} \equiv\left(1+\varpi^{k} u_{0}\right)^{\theta(s)} \equiv 1+\omega^{m}(s) \varpi^{k} u_{0} \quad\left(\bmod \varpi^{k+1}\right)
$$

which implies $k \equiv m(\bmod p-1)$ and $\alpha_{\theta}=1+\varpi^{k} u, k \in\{m, m+p-1, \ldots\}$; whence the first claim. The $p$-primarity condition for $\alpha_{\theta}$ is $\alpha_{\theta} \equiv 1\left(\bmod \varpi^{p}\right)$ giving the obvious direction " $\alpha_{\theta} p$-primary $\Rightarrow \alpha_{\theta} \equiv 1(\bmod p)$ " since $\left(\varpi^{p}\right)=(p \varpi)$.
Suppose $\alpha_{\theta} \equiv 1\left(\bmod \varpi^{p-1}\right)$; so $k=m$ does not work in the writing $\alpha_{\theta}=1+\varpi^{k} u$ since $m \leq p-2$, and necessarily $k$ is at least $m+p-1 \geq p+1$, because $m \geq 2$ (which is also the local $p$ th power condition).

## 3. Abelian $\boldsymbol{p}$-ramification

Let's give an overview of the theory of abelian $p$-ramification, which is not our main purpose, but the natural framework for Vandiver's conjecture and Gauss sums.
3.1. Vandiver's conjecture and abelian $p$-ramification. Let $U$ be the group of principal local units at $p$ of $K$ and let $\bar{E}$ be the closure of the image of $E$ in $U$. Let $\mathcal{T}$ be the torsion group of the Galois group of the maximal abelian $p$-ramified (i.e., unramified outside $p$ ) pro- $p$-extension $H^{\text {pr }}$ of $K$. This extension contains the $p$-Hilbert class field $H$ and the compositum $\widetilde{K}$ of the $\mathbb{Z}_{p}$-extensions of $K$. In the case of $K=\mathbb{Q}\left(\mu_{p}\right)$, the theory is summarized by the following exact sequences (since Leopoldt's conjecture holds for abelian fields):

$$
\begin{aligned}
& 1 \longrightarrow \operatorname{tor}_{\mathbb{Z}_{p}}(U / \bar{E}) \longrightarrow \mathcal{T} \longrightarrow \widetilde{\mathcal{C}} \longrightarrow 1 \\
& 1 \longrightarrow \operatorname{tor}_{\mathbb{Z}_{p}}(U) / \operatorname{tor}_{\mathbb{Z}_{p}}(\bar{E})=1 \longrightarrow \operatorname{tor}_{\mathbb{Z}_{p}}(U / \bar{E}) \xrightarrow{\log } \mathcal{R} \longrightarrow 0,
\end{aligned}
$$

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

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

For more information, see [15, 17, 19]. We then have $\operatorname{Gal}\left(H^{\mathrm{pr}} / K\right) \simeq \Gamma \oplus \mathcal{T} \simeq \mathbb{Z}_{p}^{\frac{p+1}{2}} \oplus \mathcal{T}$ where $\Gamma:=\operatorname{Gal}(\widetilde{K} / K)$ is such that $\Gamma_{+}=\Gamma_{1} \simeq \mathbb{Z}_{p}$ and $\Gamma_{-} \simeq \mathbb{Z}_{p}[G]_{-}$giving $\Gamma_{\theta} \simeq \mathbb{Z}_{p}$ for all odd $\theta$.
Write $\mathcal{T}=\mathcal{T}_{+} \oplus \mathcal{T}_{-}$and define $H_{-}^{\mathrm{pr}} \subseteq H^{\mathrm{pr}}$ (fixed by $\left.\operatorname{Gal}\left(H^{\mathrm{pr}} / K\right)_{+}\right)$, then $H_{+}^{\mathrm{pr}} \subseteq H^{\mathrm{pr}}$ (fixed by $\left.\operatorname{Gal}\left(H^{\mathrm{pr}} / K\right)_{-}\right)$. Thus $\operatorname{Gal}\left(H_{+}^{\mathrm{pr}} / K\right) \simeq \mathbb{Z}_{p} \oplus \mathcal{T}_{+}$and $\operatorname{Gal}\left(H_{-}^{\mathrm{pr}} / K\right) \simeq \mathbb{Z}_{p}^{\frac{p-1}{2}} \oplus \mathcal{T}_{-}$.
One defines in the same way the fields $H_{\theta}^{\mathrm{pr}}$ for which $\operatorname{Gal}\left(H_{\theta}^{\mathrm{pr}} / K\right) \simeq \Gamma_{\theta} \oplus \mathcal{T}_{\theta}$ (reduced to $\mathcal{T}_{\theta}$, finite, for all $\theta \in \mathscr{X}_{+}$). We have $H_{\theta} \subset H_{\theta}^{\mathrm{pr}}$ in terms of components of $H$.
Note that $H_{+}^{\mathrm{pr}} / K$ is decomposed over $K_{+}$to give the maximal abelian $p$-ramified pro- $p$ extension of $K_{+}$.

Theorem 3.1. For all irreducible p-adic character $\theta$ of $K$, we have $\operatorname{rk}_{p}\left(\mathcal{T}_{\theta^{*}}\right)=\operatorname{rk}_{p}\left(\mathcal{C l}_{\theta}\right)$.

Proof. We will give an outline of this famous reflection result as follows from classical Kummer duality between radicals and Galois groups (see, e.g., [15, Theorem I.6.2 \& Corollary I.6.2.1]), using the fact that $K(\sqrt[p]{\beta}) / K, \beta \in K^{\times}$, is $p$-ramified if and only if $(\beta)=\mathfrak{p}^{e} \cdot \mathfrak{A}^{p}$, $e \geq 0, \mathfrak{A} \in I$. We shall have to take the $\theta$ or $\theta^{*}$-components for each object considered in $K^{\times} \otimes \mathbb{Z}_{p}, I \otimes \mathbb{Z}_{p} \ldots$, modulo $p$ th powers:
Let $\theta$ be even. The Kummer radical of the compositum of the cyclic extensions of degree $p$ of $K$, contained in $H_{\theta^{*}}^{\mathrm{pr}}$, is generated (modulo $K^{\times p}$ ) by the part $E_{\theta}$ of real units, giving a $p$-rank 1 for $\theta \neq 1$ (and 0 for $\theta=1$ ), by $p$ (of character 1 ), and by the pseudo-units $\alpha_{\theta}$ comming from the elements of order $p$ of $\mathcal{C}_{\theta}$, which gives a radical of $p$-rank $1+\mathrm{rk}_{p}\left(\mathcal{C}_{\theta}\right)$. Since $\operatorname{rk}_{p}\left(\operatorname{Gal}\left(H_{\theta^{*}}^{\mathrm{pr}} / K\right)\right)=1+\operatorname{rk}_{p}\left(\mathcal{T}_{\theta^{*}}\right)$, we get $\operatorname{rk}_{p}\left(\mathcal{T}_{\theta^{*}}\right)=\operatorname{rk}_{p}\left(\mathcal{C l}_{\theta}\right)$. Similarly, we have $\mathrm{rk}_{p}\left(\mathcal{T}_{\theta}\right)=\mathrm{rk}_{p}\left(\mathcal{C l}_{\theta^{*}}\right)$.

Corollary 3.2. One has $\mathcal{T}_{1}=\mathcal{T}_{\omega}=\mathcal{C l}_{\omega}=\mathcal{C l}_{1}=1$ and for all $\chi \in \mathscr{X}_{+}$, we have $\mathcal{R}_{\chi^{*}}=1$ and $\mathcal{T}_{\chi^{*}}=\widetilde{\mathscr{C}}_{\chi^{*}} \subseteq \mathcal{C l}_{\chi^{*}}$, which establishes the Hecke reflection theorem or Leopoldt spiegelungssatz $\operatorname{rk}_{p}\left(\mathcal{C l}_{\chi^{*}}\right)=\operatorname{rk}_{p}\left(\mathcal{C l}_{\chi}\right)+\delta_{\chi}, \delta_{\chi} \in\{0,1\}$ since $\Gamma_{\chi^{*}} \simeq \mathbb{Z}_{p}$ (particular case of [15, Theorem II.5.4.5, 5.4.9.2]).

Remark 3.3. (i) One says that $K$ is $p$-rational if $\mathcal{T}=1$ (same definition for any number field fulfilling the Leopoldt conjecture at $p$; see $[17,21]$ for more details and programs testing the $p$-rationality of any number field). For the $p$ th cyclotomic field $K$ this is equivalent to its " $p$-regularity" in the more general context of "regular kernel" given in [12, 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 $\alpha \in\left(K^{\times} / K^{\times p}\right)$ - such that $L_{+} K=K(\sqrt[p]{\alpha})$. Put $(\alpha)=\mathfrak{A}^{p}$, where $d(\mathfrak{A}) \in \mathcal{C} l_{-}$; moreover $\mathfrak{A}$ is not principal, otherwise $\alpha$ should be, up to a $p$ th power factor, a unit $\varepsilon$ such that $\varepsilon^{1+s_{-1}}=1$, which gives $\varepsilon \in \mu_{p}$ (absurd). In the same way, if $G$ operates via $\chi$ on $\operatorname{Gal}\left(L_{+} / K_{+}\right)$then by Kummer duality $G$ operates via $\chi^{*}$ on $\langle\alpha\rangle K^{\times p} / K^{\times p}$.
(iii) As explained in the Introduction, we shall prove in Section 4 that such pseudo-units $\alpha$ may be found by means of twists $\mathrm{g}_{c}(\ell):=\tau(\psi)^{c-\sigma_{c}}$ associated to primes $\ell \equiv 1(\bmod p)$ and Artin automorphisms $\sigma_{c}$.
3.2. Vandiver's conjecture and Gauss sums. Recall the formula [15, Corollary III.2.6.1]:

$$
\# \mathcal{T}_{-}=\frac{\# \mathbb{C l}_{-}}{\#\left(\mathbb{Z}_{p} \log (I) / \mathbb{Z}_{p} \log (U)\right)_{-}}
$$

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

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

The following reasonning (from $[14, \S 3]$ ) gives another interpretation of the result of Iwasawa [28]. 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 $S . e_{\chi^{*}}=B_{1,\left(\chi^{*}\right)^{-1}} . e_{\chi^{*}} \in \mathbb{Z}_{p}[G]$ for all $\chi \in \mathscr{X}_{+}$; then $\chi^{*}=\omega^{p-n}$ for which $\# C_{\chi^{*}}$ corresponds to the ordinary Berrnoulli numbers $B_{n}$ giving the "exponents of $p$-irregularity" $n$ for $B_{n} \equiv 0$ $(\bmod p)($ see Definitions 1.3 (vii)).

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

$$
\begin{equation*}
\tau(\psi):=-\sum_{x \in \mathbb{F}_{\ell}^{\times}} \psi(x) \xi_{\ell}^{x} \in \mathbb{Z}\left[\mu_{p \ell}\right] . \tag{3}
\end{equation*}
$$

Lemma 3.4. We have $\tau(\psi)^{\sigma_{a}}=\psi(a)^{-a} \tau\left(\psi^{a}\right)$, where $\sigma_{a}$ is the Artin automorphism attached to a in $\operatorname{Gal}\left(\mathbb{Q}\left(\mu_{p \ell}\right) / \mathbb{Q}\right)$, and $\tau(\psi)^{p} \in \mathbb{Z}\left[\zeta_{p}\right]$; then $\tau(\psi) \equiv 1\left(\bmod \mathfrak{p} \mathbb{Z}\left[\mu_{p \ell}\right]\right)$.
Proof. By definition of $\sigma_{a}$, one has $\tau(\psi)^{\sigma_{a}}=-\sum_{x \in \mathbb{F}_{\ell}^{\times}} \psi(x)^{a} \xi_{\ell}^{a x}=-\psi^{a}\left(a^{-1}\right) \sum_{y \in \mathbb{F}_{\ell}^{\times}} \psi^{a}(y) \xi_{\ell}^{y}$;
whence the second claim taking $\sigma_{a} \in \operatorname{Gal}\left(\mathbb{Q}\left(\mu_{p \ell}\right) / K\right)$ (i.e., $a \equiv 1(\bmod p)$ ).
Then $\tau(\psi) \equiv-\sum_{x \in \mathbb{F}_{\ell}^{\times}} \xi_{\ell}^{x}\left(\bmod \mathfrak{p} \mathbb{Z}\left[\mu_{p \ell}\right]\right)$; since $\ell$ is prime, $\sum_{x \in \mathbb{F}_{\ell}^{\times}} \xi_{\ell}^{x}=-1$.
We then have the fundamental classical relation in $K$ (see [52, $\S \S 6.1,6.2,15.1]$ ):

$$
\begin{equation*}
\mathfrak{L}^{p S}=\tau(\psi)^{p} \mathbb{Z}\left[\zeta_{p}\right], \tag{4}
\end{equation*}
$$

for $\mathfrak{L} \mid \ell$ such that $\psi$ is defined on the multiplicative group of $\mathbb{Z}\left[\zeta_{p}\right] / \mathfrak{L} \simeq \mathbb{F}_{\ell}$.
Remark 3.5. (i) Since various choices of $\mathfrak{L} \mid \ell, \xi_{\ell}$ and $\psi$, from a given $\ell$, correspond to Galois conjugations and/or products by a $p$ th root of unity, we denote simply $\tau(\psi)$ such a Gauss sum, where $\psi$ is for instance the canonical character of order $p$; for convenience, we shall have in mind that $\ell$ defines such a $\tau(\psi)$ (and some other objects) in an obvious way. One verifies that the forthcoming properties ( $p$-primarities, Kummer radicals...) do not depend on these choices especially because of the action of the $\theta$-components.
(ii) If we consider $\alpha:=\tau(\psi)^{p} \in K^{\times}$as the Kummer radical of the cyclic extension $M_{\ell}:=$ $K(\tau(\psi))$ of $K$, we have $\alpha^{c-s_{c}}=: \mathrm{g}_{c}(\ell)^{p}$, where $\mathrm{g}_{c}(\ell):=\tau(\psi)^{c-\sigma_{c}} \in K^{\times}$; which gives $M_{\ell}=$ $K(\sqrt[p]{\alpha})=F_{\ell} K$, where $F_{\ell}$ is the subfield of $\mathbb{Q}\left(\mu_{\ell}\right)$ of degree $p$ (the character of $\langle\alpha\rangle K^{\times p} / K^{\times p}$ is $\omega$ and that of $\operatorname{Gal}\left(M_{\ell} / K\right)$ is 1 ). Thus $p$ is unramified in $M_{\ell} / K$ (which is coherent with $\tau(\psi) \equiv 1\left(\bmod \mathfrak{p} \mathbb{Z}_{p}\left[\mu_{p \ell}\right]\right)$ implying $\left.\tau(\psi)^{p} \equiv 1\left(\bmod \mathfrak{p}^{p}\right)\right) ;$ it splits if and only if $\tau(\psi)^{p} \equiv 1$ $\left(\bmod \mathfrak{p}^{p+1}\right)$.
Taking the logarithms in (4), we obtain, for all $\chi \in \mathscr{X}_{+}$:

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

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

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

where $\mathcal{G}$ is the group generated by all the previous Gauss sums.
So, the "Vandiver conjecture at $\chi \in \mathscr{X}_{+}$" is equivalent to $\left(\mathbb{Z}_{p} \log (\mathcal{G}) / \log (U)\right)_{\chi^{*}}=1$, 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 [28].
We shall from now make the following working hypothesis which corresponds to the more subtle case for testing Vandiver's conjecture with Theorems 4.7, 4.9 (or Theorem 1.2), the case where some $\mathcal{C}_{\chi^{*}}$ are not cyclic being obvious for all the forthcoming statements, as soon as one knows that $B_{1,\left(\chi^{*}\right)^{-1}} \sim p^{e}$ gives the order of $\mathcal{C l}_{\chi^{*}}$ thus its annihilation and identities of the form $\mathfrak{a}^{p^{e}}=\left(\beta^{p}\right), \beta \in K^{\times}$. So, this will give $\mathscr{E}_{\ell}(p) \cap \mathscr{E}_{0}(p) \neq \emptyset$ for all $\ell \equiv 1(\bmod p)$ (see § 4.2):

Hypothesis 3.6 (Cyclicity hypothesis). We assume that, for all $\chi \in \mathscr{X}_{+}$, the component $\mathcal{C l}_{\chi^{*}}$ of the p-class group is cyclic (which implies the cyclicity of $\mathcal{C l}_{\chi}$ ); in other words, we restrict ourselves to the case where $\mathcal{C l}$ is $\mathbb{Z}_{p}[G]$-monogenous (cf. Definition 1.3 (viii)), giving $\mathrm{rk}_{p}\left(\mathrm{Cl}_{-}\right)=i(p)$.
3.3. Vandiver's conjecture and ray class group modulo ( $p$ ). Assume the Hypothesis 3.6 and let $\chi=\omega^{n} \in \mathscr{X}_{+}$be such that $B_{1,\left(\chi^{*}\right)^{-1}} \sim p^{e}, e \geq 1$ (i.e., $\mathcal{C l}_{\chi^{*}} \simeq \mathbb{Z} / p^{e} \mathbb{Z}$ ); thus, from (5), we have $\mathcal{T}_{\chi^{*}}=1$ (i.e., $\mathcal{C l}_{\chi}=1$ ) if and only if there exists a prime number $\ell \equiv 1$ $(\bmod p)$ such that the corresponding $\log \left(\tau(\psi)_{\chi^{*}}\right)$ generates $\log \left(U_{\chi^{*}}\right)=\log \left(1+\varpi^{p-n} \mathbb{Z}_{p}[\varpi]\right)=$ $\varpi^{p-n} \mathbb{Z}_{p}[\varpi]$ (Proposition 2.4), which indicates analytically the non-p-primarity of $\tau(\psi)_{\chi^{*}}$ in $\mathbb{Z}\left[\zeta_{p}\right]$ since $n>1$.
There is also the fact that the Gauss sums (or the $\mathrm{g}_{c}(\ell)$ ), considered modulo $p$ th powers and computed modulo $p$, are indexed by infinitely many $\ell$; in other words there are some non-obvious large periodicities in the results as $\ell$ varies since numerical data are finite in number.
This may be explained as follows (giving also an interesting criterion which will imply new heuristics):

Theorem 3.7. Let $\mathcal{C} \ell^{(p)}$ be the $p$-subgroup of the ray class group $I /\{(x), x \equiv 1(\bmod p)\}$ of modulus $p \mathbb{Z}\left[\zeta_{p}\right]$. Then for any $\chi \in \mathscr{X}_{+}$, we have (under the Hypothesis 3.6) the following properties:
(i) $\# \mathcal{C l}_{\chi *}^{(p)}=p \cdot \# \mathcal{C l}_{\chi *}$.
(ii) The condition $\mathcal{C l}_{\chi}=1$ is equivalent to the cyclicity of $\mathcal{C l}_{\chi^{*}}^{(p)}$.

Proof. Let $V:=\left\{x \in K^{\times}, x \equiv 1(\bmod \mathfrak{p})\right\}$ and $W:=\left\{x \in K^{\times}, x \equiv 1(\bmod p)\right\}$. Since $E_{\chi^{*}}=1$, we have the exact sequence (using Proposition 2.4):

$$
1 \rightarrow(V / W)_{\chi^{*}} \simeq \mathbb{F}_{p} \longrightarrow \mathcal{C l}_{\chi^{*}}^{(p)} \longrightarrow \mathcal{C l}_{\chi^{*}} \rightarrow 1
$$

giving (i). The statement (ii) is obvious if $\mathcal{C l}_{\chi^{*}}=1$. Suppose $\# \mathcal{C l}_{\chi^{*}}=p^{e}$, with $e \geq 1$.
Then $\mathcal{C} \ell_{\chi}=1$ implies $\mathcal{T}_{\chi^{*}}=1$ (from Theorem 3.1) which implies $\mathcal{C} \ell_{\chi *}^{(p)} \simeq \mathbb{Z} / p^{e+1} \mathbb{Z}$ : indeed, the $\chi^{*}$-part $H_{\chi^{*}}^{\mathrm{pr}} / K$ of the pro- $p$-extension $H^{\mathrm{pr}} / K$ is a $\mathbb{Z}_{p}$-extension, thus the $p$-ray class field corresponding to $\mathcal{C l}_{\chi^{*}}^{(p)}$, contained in $H_{\chi *}^{\mathrm{pr}}$, is a cyclic extension of $K$.
Reciprocally, if $\mathcal{C} \ell_{\chi *}^{(p)} \simeq \mathbb{Z} / p^{e+1} \mathbb{Z}, e \geq 1$ (thus $\mathcal{C l}_{\chi^{*}} \simeq \mathbb{Z} / p^{e} \mathbb{Z}$ ), there exists $\mathfrak{A}$ (whose class generates $\left.\mathcal{C l}_{\chi *}^{(p)}\right)$ such that $\mathfrak{A}_{\chi^{*}}^{p^{e}}=\left(\alpha_{\chi^{*}}\right)$ (where $\alpha_{\chi^{*}}$ is unique up to a $p$ th power since $E_{\chi^{*}}=1$ ) with $\alpha_{\chi^{*}} \equiv 1\left(\bmod \mathfrak{p}^{p-n}\right)\left(\chi=: \omega^{n}, n \in[2, p-3]\right.$ even $)$, but $\alpha_{\chi^{*}} \not \equiv 1(\bmod p)$. Note that $\operatorname{rk}_{p}\left(\mathcal{T}_{\chi}\right)=\operatorname{rk}_{p}\left(\mathcal{C l}_{\chi^{*}}\right)=1$. Thus $\alpha_{\chi^{*}}$ defines the radical of the unique $p$-ramified (but not unramified) cyclic extension of degree $p$ of $K$ decomposed over $K_{+}$into $L_{+} / K_{+}$and contained in $H_{\chi}^{\mathrm{pr}}$ (its Galois group is a quotient of order $p$ of the cyclic group $\mathcal{T}_{\chi}$ since $\Gamma_{\chi}=1$ for an even $\chi \neq 1$ ); thus $\mathcal{C} l_{\chi}=1$.

## 4. Twists of Gauss sums associated to primes $\ell \equiv 1(\bmod p)$

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

$$
\begin{equation*}
\tau(\psi):=-\sum_{x \in \mathbb{F}_{\ell}^{\times}} \psi(x) \cdot \xi_{\ell}^{x}=-\sum_{k=0}^{\ell-2} \zeta_{p}^{k} \cdot \xi_{\ell}^{g^{k}} \tag{6}
\end{equation*}
$$

4.1. Computation and properties of the twists $\mathrm{g}_{c}(\ell):=\boldsymbol{\tau}(\psi)^{c-\sigma_{c}}$. Let $c \in[2, p-2]$ be a primitive root modulo $p$; to get an integer of $K$ (a PARI/GP program in $\mathbb{Z}\left[\mu_{p \ell}\right]$ overflows as $\ell$ increases, even if $\tau(\psi)_{\chi^{*}}=\tau(\psi)^{e^{\prime}}{ }_{\chi *}$ makes sense in $\mathbb{Z}\left[\zeta_{p}\right]$, a posteriori), one uses the twist $\tau(\psi)^{c-\sigma_{c}}$, where $\sigma_{c}$ is the Artin automorphism attached to $c$ in $\operatorname{Gal}\left(\mathbb{Q}\left(\mu_{p \ell}\right) / \mathbb{Q}\right)$. We define for $\ell \in \mathscr{L}_{p}$ (cf. Lemma 3.4):

$$
\begin{equation*}
\mathrm{g}_{c}(\ell):=\tau(\psi)^{c-\sigma_{c}} \in \mathbb{Z}\left[\zeta_{p}\right] \quad \text { (see formulas (3), (4) and Remark 3.5). } \tag{7}
\end{equation*}
$$

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

$$
\mathfrak{L}^{S_{c}}=\mathrm{g}_{c}(\ell) \mathbb{Z}\left[\zeta_{p}\right] \quad \& \quad \mathfrak{L}_{\chi^{*}}^{\left(c-\chi *\left(s_{c}\right)\right) \cdot B_{1,\left(\chi^{*}\right)^{-1}}}=\mathrm{g}_{c}(\ell)_{\chi *} \mathbb{Z}\left[\zeta_{p}\right]
$$

(see Definitions 1.3), where $\mathfrak{L} \mid \ell$ in $K, S_{c}:=\left(c-s_{c}\right) \cdot S \in \mathbb{Z}[G]$ is the corresponding twist of the Stickelberger element and where $\mathrm{g}_{c}(\ell) \in \mathbb{Z}\left[\zeta_{p}\right]$. Put:

$$
\begin{equation*}
b_{c}\left(\chi^{*}\right):=\left(c-\chi^{*}\left(s_{c}\right)\right) \cdot B_{1,\left(\chi^{*}\right)^{-1}} \sim B_{1,\left(\chi^{*}\right)^{-1}}, \text { for all } \chi \in \mathscr{X}_{+} \tag{8}
\end{equation*}
$$

Then we obtain the main relation that will be of a constant use:

$$
\begin{equation*}
\mathfrak{L}_{\chi^{*}}^{b_{c}(\chi *)}=\mathrm{g}_{c}(\ell)_{\chi^{*}} \mathbb{Z}\left[\zeta_{p}\right] \tag{9}
\end{equation*}
$$

Remark 4.1. (i) In the above definition (7) of $\mathrm{g}_{c}(\ell), \tau(\psi)^{\sigma_{c}}=\tau\left(\psi^{c}\right) \cdot \psi^{-c}(c)$ (Lemma 3.4); but for all $\chi \neq 1, \mu_{p}^{e_{\chi *}}=1$, defining $\mathrm{g}_{c}(\ell)_{\chi^{*}}$ without ambiguity up to $K^{\times p}$, which does not change the $p$-primarity properties. But in some sense the best definition of the twists should be $\psi^{-c}(c) \cdot \mathrm{g}_{c}(\ell)=\psi^{-c}(c) \cdot \tau(\psi)^{c-\sigma_{c}}$.
(ii) Note that, since $\tau(\psi)^{1+s_{-1}}=\ell$, this yields $\mathrm{g}_{c}(\ell)_{\chi} \in K^{\times p}$ for all $\chi \in \mathscr{X}_{+}$.

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 $\psi^{-c}(c) \cdot \mathrm{g}_{c}(\ell) \equiv \mathrm{g}_{c}(\ell) \equiv 1(\bmod \mathfrak{p})$.

Proof. The classical formula $[52, \S 6.1]$ for Jacobi sums (with $\psi \psi^{\prime} \neq 1$ ) is:

$$
J\left(\psi, \psi^{\prime}\right):=\tau(\psi) \cdot \tau\left(\psi^{\prime}\right) \cdot \tau\left(\psi \psi^{\prime}\right)^{-1}=-\sum_{x \in \mathbb{F}_{\ell} \backslash\{0,1\}} \psi(x) \cdot \psi^{\prime}(1-x)
$$

Whence $\tau(\psi)^{c}=J_{1} \cdots J_{c-1} \cdot \tau\left(\psi^{c}\right)$, where $J_{i}=-\sum_{x \in \mathbb{F}_{\ell} \backslash\{0,1\}} \psi^{i}(x) \cdot \psi(1-x)$, thus:

$$
\tau(\psi)^{c-\sigma_{c}}=J_{1} \cdots J_{c-1} \cdot \tau\left(\psi^{c}\right) \tau(\psi)^{-\sigma_{c}}=J_{1} \cdots J_{c-1} \cdot \psi^{c}(c)
$$

from Lemma 3.4 ; then $\tau(\psi) \equiv 1\left(\bmod \mathfrak{p} \mathbb{Z}\left[\mu_{p \ell}\right]\right)$ implies the result for $\mathrm{g}_{c}(\ell)$.
Thus, in the numerical computations, we shall use the relation:

$$
\begin{equation*}
\mathrm{g}_{c}(\ell)_{\chi *}=\left(J_{1} \cdots J_{c-1}\right)_{\chi *} \text { for any } \chi \in \mathscr{X}_{+} \tag{10}
\end{equation*}
$$

The following definitions will be of constant use in the paper:
Definition 4.3 (exponents of $p$-primarity and $p$-irregularity). (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 $\mathrm{g}_{c}(\ell)_{\omega^{p-n}} \equiv 1(\bmod p)$ (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 $B_{n} \equiv 0(\bmod p)$, thus, $B_{1, \omega^{n-1}} \equiv 0(\bmod p)($ see Definitions $1.3($ vii $))$.

Remark 4.4. Let $\chi=: \omega^{n} \in \mathscr{X}_{+}$and $\ell \in \mathscr{L}_{p}$. If $\mathrm{g}_{c}(\ell)_{\chi^{*}}$ is $p$-primary $\left(n \in \mathscr{E}_{\ell}(p)\right)$ this does not give necessarily a counterexample to Vandiver's conjecture for the two following possible reasons considering $S_{c} e_{\chi *}=b_{c}\left(\chi^{*}\right) e_{\chi *}$; recall that from (8),

$$
b_{c}\left(\chi^{*}\right)=\left(c-\chi^{*}\left(s_{c}\right)\right) \cdot B_{1,\left(\chi^{*}\right)^{-1}} \sim B_{1,\left(\chi^{*}\right)^{-1}}=B_{1, \omega^{n-1}}
$$

(i) The number $b_{c}\left(\chi^{*}\right)$ is a $p$-adic unit $\left(n \notin \mathscr{E}_{0}(p)\right)$, so the radical $\mathrm{g}_{c}(\ell)_{\chi *}$ is not the $p$ th power of an ideal (thus not a pseudo-unit, even if Proposition 2.4 applies) and leads to a cyclic $\ell$-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 $x=\zeta_{11}$ ):

```
-8491773970656065727678427465045288222*x^9-1963231019856677733688722439078492228*x^8
+11757523232198873159205810348854526320*x^7-5860674150310922200348907606983566648*x^6
-644088006192816851608142123579276962*x^5-611074014289231284308386817199658010*x^4
+2673005955545675004066087284224877298*x^3+15023028737838809151251842166615658188*x^2
+1520229819300797188419125563036321734*x+17836238554732163868933693789025679469
```

for which $K(\sqrt[11]{\alpha}) / K$ is decomposed over $K_{+}$into $L_{+} / K_{+}, \ell$-ramified; then $(\alpha)$ is a product of prime ideals above $\ell\left(s=s_{2}\right):(\alpha)=\mathfrak{L}^{1+2 s+2^{2} s^{2}+2^{3} s^{3}+2^{4} s^{4}+2^{5} s^{5}+2^{6} s^{6}+2^{7} s^{7}+2^{8} s^{8}+2^{9} s^{9}}$, up to the 11 th power of an $\ell$-ideal. We get $\mathrm{N}_{K / \mathbb{Q}}(\alpha)=\ell^{275}$ 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 $b_{c}\left(\chi^{*}\right) \equiv 1(\bmod 11)$.
(ii) The number $b_{c}\left(\chi^{*}\right)$ is divisible by $p$, but the ideal $\mathfrak{L}_{\chi^{*}}$ is $p$-principal and then $\mathrm{g}_{c}(\ell)_{\chi^{*}}$ is a $p$ th power in $K^{\times}$(numerical examples in §4.4.1).
4.2. First main theorem. So, from the previous Remark 4.4, a sufficient condition for the existence of a counterexample to Vandiver's conjecture is the existence of $\chi \in \mathscr{X}_{+}$and $\ell \in \mathscr{L}_{p}$ such that the three following conditions are fulfilled:
(a) $b_{c}\left(\chi^{*}\right) \equiv 0(\bmod p)$,
(b) $\mathrm{g}_{c}(\ell)_{\chi^{*}}$ is $p$-primary,
(c) $\mathrm{g}_{c}(\ell)_{\chi^{*}}$ is not a global $p$ th power.

We make here a fundamental remark:
Remark 4.5. If $\operatorname{rk}_{p}\left(\mathcal{C l}_{\chi_{0}^{*}}\right) \geq 2$ for $\chi_{0}=\omega^{n_{0}} \in \mathscr{X}_{+}$(giving a counterexample to Vandiver's conjecture), we get, from the "Main Theorem", $\# C \mathcal{C}_{\chi_{0}^{*}} \sim b_{c}\left(\chi_{0}^{*}\right)$; then the $p$-part of $b_{c}\left(\chi_{0}^{*}\right)$ is strictely larger than the exponent of $\mathcal{C} \chi_{0}^{*}$ so that, in any relation $\mathfrak{L}_{\chi_{0}^{*}}^{b_{c}\left(\chi_{0}^{*}\right)}=\left(\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}}\right)$ where $\mathfrak{L}_{\chi_{0}^{*}}$ define a generating class of $\mathcal{C}_{\chi_{0}^{*}}$, necessarily $\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}}$ is a global $p$ th power (condition (c) is never fulfilled), whence the property $n_{0} \in \mathscr{E}_{\ell}(p) \cap \mathscr{E}_{0}(p) \neq \emptyset$ for all $\ell \in \mathscr{L}_{p}$; thus Theorems 4.7 and 4.9 will apply for trivial reasons and we can go back to the cases $\mathrm{rk}_{p}\left(\mathcal{C l}_{\chi^{*}}\right)<2$ (Hypothesis 3.6) for the reciprocal.
Lemma 4.6. Let $\chi \in \mathscr{X}_{+}$such that $\mathcal{C l}_{\chi} \neq 1$. There exists a totally split prime ideal $\mathfrak{L}$ such that $\mathfrak{L}_{\chi^{*}}$ represents a generator of $\mathcal{C l}_{\chi^{*}}$. Then $\mathfrak{L}^{S_{c} e_{\chi^{*}}}=\mathfrak{L}_{\chi^{*}}^{b_{c}(\chi *)}=\left(\alpha_{\chi^{*}}\right)$, where $\alpha_{\chi^{*}}$ is unique (up to a pth power), thus equal to $\mathrm{g}_{c}(\ell)_{\chi^{*}}$ which is p-primary and not a global pth power.
Proof. From the Chebotarev density theorem in $H / \mathbb{Q}$, there exists a prime $\ell$ and $\overline{\mathfrak{L}} \mid \ell$ in $H$ such that the Frobenius $\left(\frac{H / \mathbb{Q}}{\overline{\mathfrak{L}}}\right)$ generates the subgroup of $\operatorname{Gal}(H / K)$ corresponding to $\mathcal{C l}_{\chi^{*}}$ by class field theory. So $\ell$ splits completely in $K / \mathbb{Q}\left(\ell \in \mathscr{L}_{p}\right)$ and the ideal $\mathfrak{L}$ of $K$ under $\overline{\mathfrak{L}}$ is (as $\left.\mathfrak{L}_{\chi^{*}}\right)$ a representative of a generator of $\mathcal{C}_{\chi^{*}} \simeq \mathbb{Z}_{p} / b_{c}\left(\chi^{*}\right) \mathbb{Z}_{p}$. Then $\mathfrak{L}_{\chi^{*}}^{b_{c}\left(\chi^{*}\right)}=\left(\alpha_{\chi^{*}}\right)$ where $\alpha_{\chi^{*}} \notin K^{\times p} ; \alpha_{\chi^{*}}$ is unique since $E_{\chi^{*}}=1$ for $\chi^{*} \neq \omega$. In terms of Gauss sums, $\mathfrak{L}_{\chi^{*}}^{b_{c}\left(\chi^{*}\right)}=\left(\mathrm{g}_{c}(\ell)_{\chi^{*}}\right)$, thus $\alpha_{\chi^{*}}=\mathrm{g}_{c}(\ell)_{\chi^{*}}$. The $p$-primarity of $\alpha_{\chi^{*}}$ is necessary to obtain the unique (still thanks to Hypothesis 3.6) unramified Kummer extension $K\left(\sqrt[p]{\alpha_{\chi^{*}}}\right) / K$ of degree $p$, decomposed over $K_{+}$into the unramified extension $L_{+} / K_{+}$of degree $p$ in $H_{\chi}$, associated to $\mathcal{C l}_{\chi} / \mathcal{C}_{\chi}^{p}$ by class field theory, whence the $p$-primarity of $\mathrm{g}_{c}(\ell)_{\chi *}$.

Drawing the consequences of the above, we get, unconditionally, the main test for Vandiver's conjecture stated in the Introduction (Theorem 1.2 (a)). We refer to the relations (7), (8), (9) and the Definition 4.3.

Theorem 4.7. Vandiver's conjecture holds for $K=\mathbb{Q}\left(\mu_{p}\right)$ if and only if there exists $\ell \equiv 1$ $(\bmod p)$ such that $\mathscr{E}_{\ell}(p) \cap \mathscr{E}_{0}(p)=\emptyset$.

Proof. As explained in the Remark 4.5, we may assume the cyclicity Hypothesis 3.6.
Suppose $\mathscr{E}_{\ell}(p) \cap \mathscr{E}_{0}(p)=\emptyset$ and consider, for $\chi=: \omega^{n} \in \mathscr{X}_{+}$, and $\chi^{*}=\omega^{p-n}$, the relation $\mathfrak{L}_{\chi^{*}}^{b_{c}\left(\chi^{*}\right)}=\left(\mathrm{g}_{c}(\ell)_{\chi^{*}}\right)$ for the prime $\ell$ under consideration, and examine the two possibilities:
(i) If $n$ is not an exponent of $p$-irregularity (namely, $b_{c}\left(\chi^{*}\right) \not \equiv 0(\bmod p)$ or $B_{n} \not \equiv 0$ $(\bmod p))$, then $\mathcal{C l}_{\chi^{*}}=1$ and $\mathcal{C l}_{\chi}=1$ from reflection theorem (Corollary 3.2).
(ii) If $n$ is an exponent of $p$-irregularity, then $b_{c}\left(\chi^{*}\right) \sim p^{e}, e \geq 1$, giving, for some $p$-adic unit $u, \mathfrak{L}_{\chi *}^{p^{e} u}=\left(\mathrm{g}_{c}(\ell)_{\chi^{*}}\right)$ (Lemma 4.6); if $\mathfrak{L}_{\chi^{*}}^{p^{e-1} u}$ is $p$-principal, then $\mathrm{g}_{c}(\ell)_{\chi^{*}}$ is a global $p$ th power, hence $p$-primary (absurd by assumption). So $\mathfrak{L}_{\chi *}$ defines a class of order $p^{e}$ in $\mathcal{C l}_{\chi^{*}}$ for which the pseudo-unit $\mathrm{g}_{c}(\ell)_{\chi^{*}}$ is not $p$-primary by assumption; since $\operatorname{Gal}\left(H_{\chi}^{\mathrm{pr}} / K_{+}\right)=\mathcal{T}_{\chi}$ is cyclic, from relation (3.1), by Kummer duality $K\left(\sqrt[p]{g_{c}(\ell)_{\chi *}}\right)$ is the unique extension cyclic of degree $p$, decomposed over $K_{+}$and contained in $H_{\chi}^{\mathrm{pr}}$. Since it is ramified at $p$ and since $H_{\chi}^{\mathrm{pr}}$ contains the $\chi$-component of the $p$-Hilbert class field of $K_{+}$, this implies $\mathcal{C l}_{\chi}=1$.
Reciprocally, if Vandiver's conjecture holds, then $\mathcal{C l}=\mathcal{C l}_{-}$is $\mathbb{Z}_{p}[G]$-monogenous, thus the direct sum of non-trivial cyclic isotypic components generated by some p-classes $\gamma^{\left(n_{i}\right)}=$ $d\left(\mathfrak{L}_{\omega^{p-n_{i}}}^{\left(n_{i}\right)}\right) \in \mathcal{C}_{\omega^{p-n_{i}}}\left(n_{i} \in \mathscr{E}_{0}(p)\right)$ related to non-p-primary $\mathrm{g}_{c}\left(\ell^{\left(n_{i}\right)}\right)_{\omega^{p-n_{i}}}$; thus there exists, from density theorem, $\ell \in \mathscr{L}_{p}$ and $\mathfrak{L} \mid \ell$ such that $d(\mathfrak{L})_{\omega^{p-n_{i}}}=\gamma^{\left(n_{i}\right)}$ for all $i$ (e.g., $\mathfrak{L}=$ $\left.(z) \cdot \prod_{i} \mathfrak{L}_{\omega^{p-n_{i}}}^{\left(n_{i}\right)}\right)$. So each $\mathrm{g}_{c}(\ell)_{\omega^{p-n_{i}}}=\mathrm{g}_{c}\left(\ell^{\left(n_{i}\right)}\right)_{\omega^{p-n_{i}}}$ (up to a $p$ th power) is non-p-primary, whence $\mathscr{E}_{\ell}(p) \cap \mathscr{E}_{0}(p)=\emptyset$ for this prime $\ell$.

Corollary 4.8. 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., $\left.\mathscr{E}_{\ell}(p)=\emptyset\right)$, then the Vandiver conjecture holds for $p$.
4.2.1. Program computing $\mathscr{E}_{\ell}(\boldsymbol{p})$. For $p \in[3,199]$ and for the least $\ell \in \mathscr{L}_{p}$, the program computes $\mathrm{g}_{c}(\ell)$ in $\operatorname{Mod}(\mathrm{J}, \mathrm{P})$, with $\mathrm{P}=\operatorname{polcyclo(p),~where~} \mathrm{J}=\mathrm{J}_{1} \cdots \mathrm{~J}_{\mathrm{c}-1}$ is written in $\mathbb{Z}[x]$ modulo $p \mathbb{Z}[x] ; \mathrm{c}$ is a primitive root $(\bmod \mathrm{p})($ see the relation (10)).
For the computation of $\mathrm{J}_{\mathrm{i}}$ 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 $\mathrm{n}=2 * \mathrm{~m}$ for m in $[1,(p-3) / 2]$.
The program takes into account the relation $J^{1+s_{-1}} \equiv 1(\bmod p)$ in the action of the idempotents and drops the coefficient $\frac{1}{p-1}$ in $e_{\chi^{*}}$ (in which $\chi^{*}\left(s_{a}^{-1}\right)$ is replaced by the residue of $a^{n-1}$ modulo $p$ ), thus computes in reality $\mathrm{g}_{c}(\ell)^{-1 / 2}$ up to $p$ th powers. Then the polynomials Jj give, in the list LJ , the powers J modulo $p, j=1, \ldots, p-1$.
The result is given in

$$
\mathrm{Sn}=\prod_{a=1}^{(\mathrm{p}-1) / 2} \mathrm{~s}_{\mathrm{a}}\left(\mathrm{~J}^{\mathrm{an}}\right), \quad \text { from } \quad \mathrm{g}_{c}(\ell)_{\chi^{*}}^{-1 / 2}=\prod_{a=1}^{(p-1) / 2} s_{a}\left(\mathrm{~g}_{c}(\ell)^{\omega^{n-1}(a)}\right)
$$

(up to a $p$ th power), where $\omega^{n-1}(a) \equiv a^{n-1}(\bmod p)$ is computed in an and Jan is given by component $(\mathrm{LJ}$, an $)$. The conjugate $\mathrm{s}_{\mathrm{a}}\left(\mathrm{J}^{\mathrm{Jn}}\right)$ is computed in sJan via the conjugation $\mathrm{x} \mapsto \mathrm{x}^{\mathrm{a}}$ in Jan, whence the product in Sn (the exponents of $p$-primarity are denoted expp):
Note: To copy and past the programs in verbatim text, one must perhaps replace the symbol of power (in a^b) by the PARI/GP symbol (= that of the keyboard); otherwise the program does not work (this is due to the character font used by some Journals).


```
\(X=\operatorname{Mod}(x, P) ; e l=1\); while (isprime (el) ==0, el=el \(+2 * p\) ) ; \(g=z \operatorname{nprimroot(el);~}\)
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 ( \(\mathrm{j}=1, \mathrm{p}-1, \mathrm{Jj}=\mathrm{lift}(\mathrm{Jj} * \mathrm{~J})\); listinsert (LJ, \(\mathrm{Jj}, \mathrm{j})\) ) ;
for \((m=1,(p-3) / 2, n=2 * m ; \operatorname{Sn}=\operatorname{Mod}(1, P) ; f o r(a=1,(p-1) / 2\),
an=lift (Mod (a, p) ^(n-1)) ; Jan=component (LJ, an) ; sJan=Mod (0, P) ;
for \(\left(j=0, p-2, a j=l i f t(M o d(a * j, p)) ; s J a n=s J a n+x^{\wedge}(a j) * c o m p o n e n t(J a n, 1+j)\right)\);
Sn=Sn*sJan);if(Sn==1,print(" exponents of p-primarity: ",n))))\}
\(\mathrm{p}=3 \quad \mathrm{el}=7 \quad \mathrm{c}=2 \mathrm{~g}=3 \quad \mathrm{p}=97\) el=389 c=5 \(\mathrm{g}=2\) expp:26
\(\mathrm{p}=5 \quad \mathrm{el}=11 \quad \mathrm{c}=2 \quad \mathrm{~g}=2 \quad \mathrm{p}=101\) el=607 \(\mathrm{c}=2 \mathrm{~g}=3\) expp:10
\(\mathrm{p}=7 \quad \mathrm{el}=29 \mathrm{c}=2 \mathrm{~g}=2 \quad \mathrm{p}=103\) el=619 \(\mathrm{c}=5 \mathrm{~g}=3\)
\(\mathrm{p}=11\) el=23 c=3 g=5 expp:2
\(\mathrm{p}=13 \quad \mathrm{el}=53 \quad \mathrm{c}=2 \quad \mathrm{~g}=2\)
\(\mathrm{p}=17\) el=103 c=3 g=5
\(\mathrm{p}=19 \mathrm{el=191} \mathrm{c}=4 \quad \mathrm{~g}=19\)
\(\mathrm{p}=23\) el=47 \(\mathrm{c}=2 \quad \mathrm{~g}=5\)
\(\mathrm{p}=29\) el=59 c=2 g=2 expp:2
\(\mathrm{p}=31 \quad \mathrm{el}=311 \quad \mathrm{c}=7 \quad \mathrm{~g}=17\)
\(\mathrm{p}=37\) el=149 c=2 g=2
\(\mathrm{p}=41\) el=83 c=6 g=2
\(\mathrm{p}=43\) el=173 c=9 g=2 expp:26
\(\mathrm{p}=47\) el=283 c=2 g=3
\(\mathrm{p}=53\) el=107 c=2 g=2 expp:34,10
\(\mathrm{p}=59\) el=709 c=3 \(\mathrm{g}=2\)
\(\mathrm{p}=61\) el=367 c=2 g=6
\(\mathrm{p}=67\) el=269 c=4 g=2
\(\mathrm{p}=71\) el=569 c=2 \(\mathrm{g}=3\)
\(\mathrm{p}=73\) el=293 c=5 g=2
p=79 l=317 c=2
p=197 el=3547 c=2 g=2 expp:62
\(\mathrm{p}=83\) el=167 c=3 \(\mathrm{g}=5 \quad \mathrm{p}=199\) el=797 c=3 \(\mathrm{g}=2\)
\(\mathrm{p}=89 \mathrm{el}=179 \mathrm{c}=3 \quad \mathrm{~g}=2\)
```


4.2.2. Minimal prime $\ell \in \mathscr{L}_{p}$ such that $\mathscr{E}_{\ell}(\boldsymbol{p})=\emptyset$. 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, $\ell_{N}$ (in L with its index N ), such that $\mathscr{E}_{\ell_{N}}(p)=\emptyset$. Its existence is of course a strong conjecture, but the numerical results are extremely favorable to the existence of such primes; which strengthens the conjecture of Vandiver. Moreover, since the integer $i(p)=\# \mathscr{E}_{0}(p)$ is rather small regarding $p$, as doubtless for $\# \mathscr{E}_{\ell}(p)$, and can be both in $O\left(\frac{\log (p)}{\log (\log (p))}\right)$, the intersection $\mathscr{E}_{\ell}(p) \cap \mathscr{E}_{0}(p)$ may be easily empty if these sets are independent. The experiments give the impression that the sets $\mathscr{E}_{\ell}(p)$ are random when $\ell$ varies and have no link with $\mathscr{E}_{0}(p)$.

```
{forprime(p=3,100,c=lift(znprimroot(p));P=polcyclo(p)+Mod(0,p);
N=0;T=1;el=1;while(T==1,el=el+2*p;if(isprime(el)==1,N=N+1;g=znprimroot(el);
J=Mod(1,P);for(i=1,c-1,Ji=0;for(k=1,el-2,kk=znlog(1-g^k,g);
e=lift(Mod(kk+i*k,p));Ji=Ji-x^e);J=J*Ji);LJ=List;Jj=1;
for(j=1,p-1,Jj=lift(Jj*J);listinsert(LJ,Jj,j));T=0;for(m=1, (p-3)/2,n=2*m;
Sn=Mod(1,P);for (a=1, (p-1)/2,an=lift (Mod (a,p)^(n-1));Jan=component(LJ,an);
sJan=0;for(j=0,p-2,aj=lift(Mod(a*j,p));sJan=sJan+x^(aj)*component(Jan,1+j));
Sn=Sn*sJan);if(Sn==1,T=1;break));if(T==0,print(p," ",el," ",N);break))))}
```

For $p<400$, we only write the primes $p, \ell_{N}$ for which $N>1$, then a complete list for $p \in[409,683]$ :

| p | el | N | p | el | N | p | el | N | p | el | N | p | el | N |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| 11 | 67 | 2 | 197 | 4729 | 2 |  | 409 | 4091 | 2 | 499 | 1997 | 1 | 601 | 25243 |
| 5 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |


| 29 | 233 | 2 | 211 | 10973 | 4 | 419 | 839 | 1 | 503 | 3019 | 1 | 607 | 20639 |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| 43 | 431 | 2 | 223 | 6691 | 2 | 421 | 4211 | 1 | 509 | 4073 | 2 | 613 | 6131 |
| 53 | 743 | 2 | 227 | 5903 | 2 | 431 | 863 | 1 | 521 | 16673 | 1 | 617 | 30851 |
| 97 | 971 | 2 | 229 | 5039 | 2 | 433 | 5197 | 2 | 523 | 6277 | 2 | 619 | 17333 |
| 101 | 809 | 2 | 233 | 1399 | 2 | 439 | 4391 | 1 | 541 | 9739 | 1 | 631 | 6311 |
| 109 | 2399 | 2 | 251 | 4519 | 2 | 443 | 887 | 1 | 547 | 5471 | 1 | 641 | 1283 |
| 131 | 1049 | 3 | 277 | 4987 | 3 | 449 | 3593 | 1 | 557 | 24509 | 3 | 643 | 10289 |
| 137 | 1097 | 2 | 337 | 6067 | 3 | 457 | 21023 | 3 | 563 | 7883 | 1 | 647 | 9059 |
| 157 | 7537 | 5 | 349 | 8377 | 2 | 461 | 9221 | 2 | 569 | 6829 | 1 | 653 | 1307 |
| 163 | 5869 | 3 | 367 | 3671 | 2 | 463 | 5557 | 1 | 571 | 5711 | 1 | 659 | 1319 |
| 167 | 7349 | 3 | 383 | 16087 | 4 | 467 | 2803 | 1 | 577 | 3463 | 2 | 661 | 14543 |
| 179 | 1433 | 2 | 389 | 14783 | 2 | 479 | 3833 | 1 | 587 | 8219 | 1 | 673 | 2693 |
| 181 | 1811 | 2 | 397 | 6353 | 2 | 487 | 1949 | 1 | 593 | 1187 | 1 | 677 | 5417 |
| 193 | 1931 | 2 | 401 | 10427 | 4 | 491 | 983 | 1 | 599 | 4793 | 1 | 683 | 4099 |

The comparison with the table of exponents of $p$-irregularity does not show any relation.
4.3. Second main theorem. Let $n_{0}$ be an exponent of $p$-irregularity; put $\chi_{0}=\omega^{n_{0}}$ and let $b_{c}\left(\chi_{0}^{*}\right) \sim p^{e}, e \geq 1$. If $\mathcal{C}_{\chi_{0}^{*}}$ is not cyclic, Remark 4.5 implies $n_{0} \in \cap_{\ell \in \mathscr{L}_{p}} \mathscr{E}_{\ell}(p) \neq \emptyset$ and Theorem 4.9 will hold. Then we may assume $\mathcal{C l}_{\chi_{0}^{*}} \simeq \mathbb{Z} / p^{e} \mathbb{Z}$. We shall examine what happens when $\ell \in \mathscr{L}_{p}$ varies.
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 in the monogenous case:
(i) $\mathfrak{L}_{\chi_{0}^{*}}^{p^{e-1}}$ is $p$-principal. Since $b_{c}\left(\chi_{0}^{*}\right) \sim p^{e}, e \geq 1, \mathrm{~g}_{c}(\ell)_{\chi_{0}^{*}}$ is a global $p$ th power in $K^{\times}$, whence $\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}}$ is $p$-primary and $n_{0} \in \mathscr{E}_{\ell}(p)$, but this does not lead to an unramified cyclic extension of degree $p$ of $K_{+}$of character $\chi_{0}$;
(ii) $\mathfrak{L}_{\chi_{0}^{*}}^{p^{e-1}}$ is not $p$-principal (from density theorem, such primes $\ell$ always exist). Thus it defines a generator of $\mathcal{C} \chi_{\chi_{0}^{*}}$ and Vandiver's conjecture "holds for $\chi_{0}=\omega^{n_{0} "}$ if and only if $\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}}$ is not $p$-primary (Theorem 4.7).
If $\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}} \equiv 1(\bmod p)$ (counterexample to Vandiver's conjecture), we fix this $\ell$ once for all, and whatever the ideal $\mathfrak{L}^{\prime} \mid \ell^{\prime}, \ell^{\prime} \in \mathscr{L}_{p}$, we have $\mathfrak{L}_{\chi_{0}^{*}}^{\prime}=(z) \cdot \mathfrak{L}_{\chi_{0}^{*}}^{r}$, with $z \in K^{\times}$and $r \in\left[0, p^{e}-1\right]$, so:

$$
\mathfrak{L}_{\chi_{0}^{*}}^{p^{e} u}=\left(z^{p^{e} u}\right) \cdot \mathfrak{L}_{\chi_{0}^{*}}^{r p^{e} u} \quad \& \quad \mathrm{~g}_{c}\left(\ell^{\prime}\right)_{\chi_{0}^{*}} \equiv \mathrm{~g}_{c}(\ell)_{\chi_{0}^{*}}^{r} \equiv 1 \quad(\bmod p) .
$$

Whence, the exponent $n_{0}$ of $p$-irregularity is a common exponent of $p$-primarity for all $\ell \in \mathscr{L}_{p}$, giving $n_{0} \in \mathscr{E}_{0}(p) \cap\left(\cap_{\ell \in \mathscr{L}_{p}} \mathscr{E}_{\ell}(p)\right) \neq \emptyset$. In other words, the existence of an empty intersection $\mathscr{E}_{\ell_{1}}(p) \cap \cdots \cap \mathscr{E}_{\ell_{N}}(p)$ implies Vandiver's conjecture. We shall also prove the reciprocal, that gives the new criterion:

Theorem 4.9. Vandiver's conjecture holds if and only if there exist $N \geq 1$ and $\ell_{1}, \ldots, \ell_{N} \in$ $\mathscr{L}_{p}$ such that $\mathscr{E}_{\ell_{1}}(p) \cap \cdots \cap \mathscr{E}_{\ell_{N}}(p)=\emptyset$.
Proof. It remains to prove that Vandiver's conjecture implies such an empty intersection. Assume, on the contrary, that for all $N \geq 1$ and all sets $\left\{\ell_{1}, \ldots, \ell_{N}\right\} \subset \mathscr{L}_{p}$, one has $\mathscr{E}_{\ell_{1}}(p) \cap$ $\cdots \cap \mathscr{E}_{\ell_{N}}(p) \neq \emptyset$.
Since $\mathscr{X}_{+}$is finite, there exists such an $n_{0}$ in $\bigcap_{\ell \in \mathscr{L}_{p}} \mathscr{E}_{\ell}(p)$ (if $\cap_{\ell \in \mathscr{L}_{p}} \mathscr{E}_{\ell}(p)=\emptyset$ then for all even $n \in[2, p-3]$ there exists $\ell(n)$ such that $n \notin \mathscr{E}_{\ell(n)}(p)$ whence $\bigcap_{n \in[2, p-3] \text { even }} \mathscr{E}_{\ell(n)}(p)=\emptyset$ (absurd)). This means that for the fixed character $\chi_{0}:=\omega^{n_{0}}$, we have the property:

$$
\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}} \equiv 1(\bmod p), \text { for all } \ell \in \mathscr{L}_{p} .
$$

To simplify, put $\alpha(\ell):=\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}}$ and consider the extensions $K(\sqrt[p]{\alpha(\ell)}) / K$; these extensions, with Galois groups of character $\chi_{0}$, are decomposed over $K_{+}$into cyclic extensions $L_{+}(\ell) / K_{+}$
(possibly trivial), and are $\ell$-ramified since $(\alpha(\ell))=\mathfrak{L}_{\chi_{0}^{*}}^{b_{c}\left(\chi_{0}^{*}\right)}$ with $\alpha(\ell) \equiv 1(\bmod p)$ (nonramification at $p$ ). Examine the two possibilities about $b_{c}\left(\chi_{0}^{*}\right)$ :
(i) $b_{c}\left(\chi_{0}^{*}\right) \equiv 0(\bmod p)$. Then $\alpha(\ell)$ is, for all $\ell$, a $p$-primary pseudo-unit, and choosing $\ell$ such that $\mathfrak{L}_{\chi_{0}^{*}}$ generates $\mathcal{C}_{\chi_{0}^{*}}$ (which is cyclic since $\mathcal{C}_{\chi_{0}}=1$ ), the extension $L_{+}(\ell) / K_{+}$is unramified of degree $p$ (absurd).
(ii) $b_{c}\left(\chi_{0}^{*}\right) \not \equiv 0(\bmod p)$. Then $L_{+}(\ell) / K_{+}$is, for all $\ell$, a $\ell$-ramified degree $p$ cyclic extension of character $\chi_{0}$. We restrict ourselves to primes $\ell \not \equiv 1\left(\bmod p^{2}\right)$ and consider the $p$-ray class fields, $H_{+}(\ell)$ over $K_{+}$, of modulus $(\ell)$; we have $L_{+}(\ell) \subseteq H_{+}(\ell)$. Since $\mathcal{C l}_{+}=1$, $\operatorname{Gal}\left(H_{+}(\ell) / K_{+}\right) \simeq\left(P_{+} / P_{+}(\ell)\right) \otimes \mathbb{Z}_{p}$, where $P_{+}$is the group of principal ideals prime to $\ell$ of $K_{+}$and $P_{+}(\ell)$ the subgroup of $P_{+}$of ideals generated by an element $x \equiv 1(\bmod \ell)$.
From the $G$-modules exact sequence $1 \rightarrow E_{+} / E_{+}(\ell) \rightarrow \underset{\mathfrak{L}_{+} \mid \ell}{\bigoplus_{\ell}} \mathbb{F}_{\ell}^{\times} \rightarrow P_{+} / P_{+}(\ell) \rightarrow 1$, where $E_{+}(\ell):=\left\{\varepsilon \in E_{+}, \varepsilon \equiv 1(\bmod \ell)\right\}$, we get $\left(\right.$ for $\left.\ell \not \equiv 1\left(\bmod p^{2}\right)\right)$ :

$$
1 \rightarrow\left(E_{+} / E_{+}(\ell)\right)_{\chi_{0}} \longrightarrow(\mathbb{Z} / p \mathbb{Z})_{\chi_{0}} \longrightarrow \operatorname{Gal}\left(H_{+}(\ell) / K_{+}\right)_{\chi_{0}} \rightarrow 1
$$

Since $\operatorname{Gal}\left(H_{+}(\ell) / K_{+}\right)_{\chi_{0}}$ is, at least, of order $p$, the generating $\chi_{0^{-}}$unit, $\varepsilon_{\chi_{0}}=: \varepsilon$, is in $E_{+}(\ell)_{\chi_{0}}$, thus locally a $p$ th power at $\ell$, for all $\ell \in \mathscr{L}_{p}, \ell \not \equiv 1\left(\bmod p^{2}\right)$. Thus $\ell$ totally splits in $K(\sqrt[p]{\varepsilon}) / K$. Let $M$ be the compositum $K(\sqrt[p]{\varepsilon}) \cdot K_{1}$, where $K_{1}=\mathbb{Q}\left(\mu_{p^{2}}\right)$; this Galois field $M$ only depends on $p$ and $\chi_{0}$ and the primes $\ell \not \equiv 1\left(\bmod p^{2}\right)$ are inert in $K_{1} / K$. Then choose $\ell$ such that the decomposition group of $\mathcal{L} \mid \ell$ does not fix $K(\sqrt[p]{\varepsilon})\left(\right.$ since $\operatorname{Gal}(M / K) \simeq(\mathbb{Z} / p \mathbb{Z})^{2}$, this allows $p-1$ possibilities). Thus $\ell$ is inert in $K(\sqrt[p]{\varepsilon}) / K$ (contradiction).
Whence the reciprocal.
Remark 4.10. This theorem suggests that if the sets $\mathscr{E}_{\ell}(p)$ are random when $\ell$ varies and independent, the (conjectural) triviality of $\mathcal{C l}_{+}$is a consequence of a natural $p$-adic property of Gauss sums and the statement does exist with $N=1$.
On the contrary, the structure of $\mathrm{Cl}_{-}$is independent of the Gauss sums because the even components $\mathrm{g}_{c}(\ell)_{\chi}$ are global $p$ th powers for all $\ell \in \mathscr{L}_{p}$ (Remark 4.1 (ii)) and do not yield any obstruction! Thus the cases of non-triviality of $\mathcal{C l}_{-}$may follow standard probabilities under the monogenous case.
4.4. Study of the case $\boldsymbol{p}=\mathbf{3 7}$. So it is fundamental to see if the sets $\mathscr{E}_{\ell}(p)$ are independent (or not) of the choice of $\ell \in \mathscr{L}_{p}$ for $\mathscr{E}_{0}(p) \neq \emptyset$. We analyse the case of $p=37\left(n_{0}=32\right)$ giving $\# \mathscr{C}_{\omega^{5}}=37$ and compute (in expp) the sets $\mathscr{E}_{\ell}(37)$ when $\ell \in \mathscr{L}_{37}$ varies. If $n_{0} \in \mathscr{E}_{\ell}(37)$, this means that $\mathfrak{L}_{\chi^{*}}$ is necessarily 37-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,next);g=znprimroot(el);
print("el=",el," g=",lift(g));J=1;for(i=1,c-1,Ji=0;for(k=1,el-2,kk=znlog(1-g^k,g);
e=lift(Mod(kk+i*k,p));Ji=Ji-X^e);J=J*Ji);LJ=List;Jj=1;for(j=1,p-1,Jj=lift(Jj*J);
listinsert(LJ, Jj,j));for(m=1, (p-3)/2,n=2*m;Sn=Mod(1,P);for(a=1,(p-1)/2,
an=lift(Mod(a,p)^(n-1));Jan=component(LJ,an);sJan=Mod(0,P);
for(j=0,p-2,aj=lift(Mod(a*j,p));sJan=sJan+x^(aj)*component(Jan, 1+j));
Sn=Sn*SJan);if(Sn==1,print(" exponent of p-primarity: ",n))))}
el=149 g=2 el=3331 g=3 expp: 22
el=223
el=593
el=1259 g=2
el=1481
el=1777
el=1999 g=3
el=1999 
=3701
el=3923
g=2
el=4219 g=2 expp: 18,16
expp: 30
el=4441 g=21
el=4663 g=3
el=5107 g=2
el=5477 g=2
```

TEST OF VANDIVER'S CONJECTURE WITH GAUSS SUMS

| el=2591 | $\mathrm{g}=7$ | expp: 34 | el=6143 | $\mathrm{g}=5$ | expp: | 28 |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| el=2887 | $\mathrm{g}=5$ |  | el=6217 | $\mathrm{g}=5$ |  |  |
| el=3109 | $\mathrm{g}=6$ |  | el=6661 | $\mathrm{g}=6$ |  |  |
| el $=3257$ | $\mathrm{g}=3$ |  | el=6883 | $\mathrm{g}=2$ |  |  |
| el=742073 | $\mathrm{g}=3$ | expp: 12 | el=768343 | $\mathrm{g}=11$ | expp: |  |
| el=742369 | $\mathrm{g}=7$ |  | el=768491 | $\mathrm{g}=10$ |  |  |
| el=742591 | $\mathrm{g}=3$ |  | el=768787 | $\mathrm{g}=2$ | expp: | 20 |
| el=743849 | $\mathrm{g}=3$ |  | el=769231 | $\mathrm{g}=11$ | expp: | 24 |
| el=743923 | $\mathrm{g}=3$ | expp: 16 | el=769453 | $\mathrm{g}=2$ | expp: | 30 |
| el=744071 | $\mathrm{g}=22$ |  | el=772339 | $\mathrm{g}=3$ |  |  |
| el=744811 | $\mathrm{g}=10$ |  | el=773153 | $\mathrm{g}=3$ | expp: | 14 |
| el=744959 | $\mathrm{g}=13$ | expp: 10 | el=774337 | $\mathrm{g}=5$ | expp: | 28 |
| el=745033 | $\mathrm{g}=10$ | expp: 16 | el=774929 | $\mathrm{g}=3$ | expp: | 18 |
| el=745181 | $\mathrm{g}=2$ |  | el=775669 | $\mathrm{g}=10$ | expp: | 18 |
| el=745477 | $\mathrm{g}=2$ |  | el=776483 | $\mathrm{g}=2$ |  |  |
| el=745699 | $\mathrm{g}=2$ |  | el=776557 | $\mathrm{g}=2$ | expp: | 20 |
| el=746069 | $\mathrm{g}=2$ |  | el=777001 | $\mathrm{g}=31$ | expp: | 18,28 |
| el=746957 | $\mathrm{g}=2$ |  | el=778111 | $\mathrm{g}=11$ |  |  |
| el=747401 | $\mathrm{g}=3$ |  | el=778333 | $\mathrm{g}=2$ | expp: | 28 |
| el=747919 | $\mathrm{g}=3$ |  | el=778777 | $\mathrm{g}=5$ |  |  |
| el=748807 | $\mathrm{g}=6$ | expp: 22 | el=779221 | $\mathrm{g}=2$ |  |  |
| el=749843 | $\mathrm{g}=2$ | expp: 34 | el=779591 | $\mathrm{g}=7$ |  |  |
| el=750287 | $\mathrm{g}=5$ |  | el=779887 | $\mathrm{g}=10$ | expp: | 18 |
| el=750509 | $\mathrm{g}=2$ | expp: 14,22 | el=780257 | $\mathrm{g}=3$ | expp: | 8 |
| el=751027 | $\mathrm{g}=3$ |  | el=780553 | $\mathrm{g}=10$ |  |  |
| el=751841 | $\mathrm{g}=3$ | expp: 14,16,24 | el=781367 | $\mathrm{g}=5$ | expp: | 34 |
| el=752137 | $\mathrm{g}=10$ | expp: 8 | *el=781589 | e | p: 32 |  |
| el=752359 | $\mathrm{g}=3$ | expp: 18 | el=782107 | $\mathrm{g}=2$ |  |  |
| el=752581 | $\mathrm{g}=2$ | expp: 16 | el=782329 | $\mathrm{g}=13$ | expp: |  |
| el=752803 | $\mathrm{g}=2$ | expp: 22,32 | el=782921 | $\mathrm{g}=3$ | expp: | 20 |
| el=753617 | $\mathrm{g}=3$ |  | el=783143 | $\mathrm{g}=5$ |  |  |
| el=753691 | $\mathrm{g}=11$ | expp: 16 | el=783661 | $\mathrm{g}=2$ |  |  |
| el=753839 | $\mathrm{g}=7$ | expp: 4,22 | el=784327 | $\mathrm{g}=3$ |  |  |
| el=754283 | $\mathrm{g}=2$ |  | el=784697 | $\mathrm{g}=3$ |  |  |
| el=755171 | $\mathrm{g}=6$ |  | el=784919 | $\mathrm{g}=7$ |  |  |
| el=755393 | $\mathrm{g}=3$ | expp: 22 | el=785363 | $\mathrm{g}=2$ |  |  |
| el=756281 | $\mathrm{g}=3$ | expp: 2 | el=786251 | $\mathrm{g}=2$ |  |  |
| el=756799 | $\mathrm{g}=15$ | expp: 18 | el=786547 | $\mathrm{g}=2$ |  |  |
| el=757243 | $\mathrm{g}=2$ |  | el=787139 | $\mathrm{g}=2$ | expp: | 20 |
| el=757909 | $\mathrm{g}=2$ | expp: 16 | el=787361 | $\mathrm{g}=6$ |  |  |
| el=758279 | $\mathrm{g}=7$ |  | el=787879 | $\mathrm{g}=6$ | expp: | 10,18,20 |
| el=758501 | $\mathrm{g}=2$ | expp: 18 | el=788027 | $\mathrm{g}=2$ | expp: | 34 |
| el=759019 | $\mathrm{g}=2$ |  | el=789137 | $\mathrm{g}=3$ | expp: | 24 |
| el=759167 | $\mathrm{g}=5$ | expp: 12 | el=790099 | $\mathrm{g}=2$ |  |  |
| el=759463 | $\mathrm{g}=3$ |  | el=791209 | $\mathrm{g}=7$ |  |  |
| el=759833 | $\mathrm{g}=3$ | expp: 4 | el=791431 | $\mathrm{g}=12$ |  |  |
| el=760129 | $\mathrm{g}=11$ |  | el=791801 | $\mathrm{g}=3$ |  |  |
| el=760499 | $\mathrm{g}=2$ |  | *el=792023 | $\mathrm{g}=5$ | expp: | 32 |
| el=762053 | $\mathrm{g}=2$ |  | el=792689 | $\mathrm{g}=3$ |  |  |
| el=762571 | $\mathrm{g}=10$ |  | el=793207 | $\mathrm{g}=5$ |  |  |
| el=763237 | $\mathrm{g}=2$ |  | el=795427 | $\mathrm{g}=2$ |  |  |
| el=764051 | $\mathrm{g}=2$ |  | *el=795649 | $\mathrm{g}=22$ | expp: | 2,32 |
| el=764273 | $\mathrm{g}=3$ |  | el=795797 | $\mathrm{g}=2$ |  |  |
| el=764717 | $\mathrm{g}=2$ | expp: 2 | el=795871 | $\mathrm{g}=3$ |  |  |
| el=765383 | $\mathrm{g}=5$ |  | el=796759 | $\mathrm{g}=3$ |  |  |
| el=765827 | $\mathrm{g}=2$ | expp: 34 | el=796981 | $\mathrm{g}=7$ |  |  |
| el=766049 | $\mathrm{g}=3$ | expp: 22 | el=797647 | $\mathrm{g}=3$ |  |  |
| el=766937 | $\mathrm{g}=3$ | expp: 34 | el=797869 | $\mathrm{g}=10$ |  |  |


| el=767381 | $\mathrm{g}=2$ | expp: 18 | el=798461 | $\mathrm{g}=2$ |  |
| :--- | :--- | :--- | :--- | :--- | :--- |
| el=767603 | $\mathrm{g}=5$ | expp: 34 | el=798757 | $\mathrm{g}=2$ |  |
| el=767677 | $\mathrm{g}=5$ |  | el=800089 | $\mathrm{g}=7$ | 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 $\chi^{*}=\omega^{7}\left(\chi=\omega^{30} \neq \omega^{32}\right)$. Theorem 4.9 applies at will.
It remains to give statistics about the $p$-principality (or not) of the $\mathfrak{L}_{\chi_{0}^{*}}$ when $\ell \in \mathscr{L}_{p}$ varies. For $p=37, \mathfrak{L}_{\chi_{0}^{*}}$ is 37 -principal if and only if $\mathfrak{L}$ is principal since the class number of $K$ is $h=37$.
4.4.1. 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 $K$. We only write the cases $\mathscr{E}_{\ell}(37) \neq \emptyset$ :

```
{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,next);
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))))}
\begin{tabular}{|c|c|c|c|}
\hline el=1481 & expp: 30 & el=56167 & expp: 10,14,26 \\
\hline el=2591 & expp: 34 & \(e l=57203\) & expp: 34 \\
\hline el=3331 & expp: 22 & el=58313 & expp: 28 \\
\hline \(e l=4219\) & expp: 16,18 & \(e l=58757\) & expp: 16,18 \\
\hline el=6143 & expp: 28 & el=58831 & expp: 24,30 \\
\hline el=7993 & expp: 16,20 & el=59497 & expp: 28 \\
\hline el=8363 & expp: 8 & el=61051 & expp: 10 \\
\hline el=9769 & expp: 20 & el=62383 & expp: 2 \\
\hline el=10657 & expp: 4,18,26 & el=62753 & expp: 2 \\
\hline el=12433 & expp: 20 & el=63493 & expp: 2 \\
\hline el=13099 & expp: 28 & el=64381* & expp: 6,32 [ \(\left.\mathrm{x}^{\wedge} 20+\mathrm{x}^{\wedge} 9+\mathrm{x}\right]\) \\
\hline \(e l=14431\) & expp: 4,14,22 & el=66749 & expp: 30 \\
\hline el=17021 & expp: 6 & el=67489* & expp: 30,32 [ \(\left.x^{\wedge} 24-x^{\wedge} 3-x^{\wedge} 2\right]\) \\
\hline el=17909 & expp: 30 & el=67933 & expp: 6 \\
\hline el=18131 & expp: 22 & el=68821* & expp: 32 [ \(\left.\mathrm{x}^{\wedge} 15-\mathrm{x}^{\wedge} 9+\mathrm{x}^{\wedge} 4\right]\) \\
\hline el=19463 & expp: 6 & el=69931 & expp: 12 \\
\hline el=20129 & expp: 6 & el=71411 & expp: 4 \\
\hline el=21017 & expp: 2,4 & \(\mathrm{el}=72817\) & expp: 28 \\
\hline el=21313 & expp: 18 & el=74149 & expp: 2 \\
\hline el=21757 & expp: 8 & el=75407 & expp: 10 \\
\hline el=22349 & expp: 8 & el=75629 & expp: 12, 20 \\
\hline el=23459 & expp: 6 & el=76961 & expp: 14 \\
\hline el=23977 & expp: 26 & el=78737 & expp: 28 \\
\hline el=25087 & expp: 26 & el=79181 & expp: 10 \\
\hline el=25457 & expp: 30 & el=80513 & expp: 16, 26 \\
\hline el=29009 & expp: 8,24 & el=81031 & expp: 18, 34 \\
\hline el=30859 & expp: 2 & el=82067 & expp: 34 \\
\hline el=32783* & expp: 32 [ \(\left.x^{\wedge} 11+x^{\wedge} 3+x\right]\) & el=83621 & expp: 34 \\
\hline el=33301 & expp: 30 & el=83843 & expp: 2 \\
\hline el=33967 & expp: 26 & el=84731 & expp: 6 \\
\hline \(e l=36187\) & expp: 8 & el=85027 & expp: 26 \\
\hline
\end{tabular}
```

| 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 |

Give some examples ( $\mathfrak{L}^{1+s_{-1}}$ is always principal giving an easy characterization):
(ii) Non-principal case $\mathfrak{L} \mid 149$. The instruction bnfisintnorm $\left(\mathrm{K}, 149^{\mathrm{k}}\right)$ :
$\{\mathrm{P}=\mathrm{polcyclo}(37) ; \mathrm{K}=\operatorname{bnfinit}(\mathrm{P}, 1)$; for $(\mathrm{k}=1,2$, 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
```

(i) Principal case $\mathfrak{L} \mid 32783$. The principal $\mathfrak{L}$ are rare (which comes from density theorems); the first one is $\mathfrak{L}=\left(\zeta_{37}^{11}+\zeta_{37}^{3}+\zeta_{37}\right)$ where $\ell=32783$. Thus in that case, in the relation $\mathfrak{L}_{\chi_{0}^{*}}^{b_{c}\left(\chi_{0}^{*}\right)}=\left(\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}}\right)$, the number $\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}}$ must be a global 37 th power (which explains that one shall find the exponent of 37 -primarity $n_{0}=32$ equal to that of 37 -irregularity in the table); unfortunately, the data are too large to be given.
Nevertheless, the reader can easily compute
factor(norm $(S n))=32783^{37 \cdot 16 \cdot 9}$ and use $K=\operatorname{bnfinit}(P, 1)$;idealfactor(K, Sn),
which gives the 37 th power of $\mathfrak{L} \mid 32783$.
We obtain the following excerpts of the table (up to $10^{6}$ ) of principal cases:

| 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 |

4.4.2. 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 $\ell$, is counted in the ( $n / 2$ )th component of the list Eel).

```
{p=37;c=lift(znprimroot(p));P=polcyclo(p)+Mod(0,p);X=Mod(x,P);Nel=0;Npp=0;Eel=List;
for(j=1,(p-3)/2,listput(Eel, 0,j));for(i=1,1000,el=1+2*i*p;if(isprime(el)!=1,next);
g=znprimroot(el);Nel=Nel+1;J=1;for(i=1,c-1,Ji=0;for(k=1,el-2,kk=znlog(1-g^k,g);
e=lift(Mod(kk+i*k,p));Ji=Ji-X^e);J=J*Ji);LJ=List;Jj=1;for(j=1,p-1,Jj=lift(Jj*J);
listinsert(LJ, Jj,j));for(m=1, (p-3)/2,n=2*m;Sn=Mod(1,P);for(a=1, (p-1)/2,
an=lift(Mod (a,p)^(n-1));Jan=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 $\ell_{i}$ 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 $\ell_{i}$ (in el). In some cases, a prime $\ell$ gives rise to several exponents of $p$-primarity
(i) 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]
30151427 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]
30301429 1420949 [83,95,84,91,80,80,86,83,92,83,98,76,83,78,86,75,76]
30321430 1421911 [83,95,85,91,80,80,86,83,92,83,98,76,83,78,86,75,76]
30331431 1422133 [83,95,86,91,80,80,86,83,92,83,98,76,83,78,86,75,76]
3042 1432 1428127 [83,96,86,91,80,80,86,83,92,83,98,76,83,78,86,75,76]
3889 1819 1863913[106,114,108,113,99,111,115,100,117,113,116,93,103,97,108,103,103]
3894 1820 1865911[106,114,108,114,99,111,115,100,117,113,116,93,103,97,108,103,103]
38981821 1868501[106,114,108,114,100,111,115,100,117,113,116,93,103,97,108,103,103]
3900 1822 1869389[106,114,108,114,100,112,115,100,117,113,116,93,103,97,108,103,103]
3900 1823 1869389[106,114,108,114,100,112,115,101,117,113,116,93,103,97,108,103,103]
3900 1824 1869389[106,114, 108,114,100,112,115,101,117,113,116,93,104,97,108,103,103]
```

The penultimate column corresponds to the exponent of 37 -irregularity $n_{0}=32$; since there is no counterexamples to Vandiver's conjecture, when this component increases, this means that the new $\ell$ gives rise to a principal $\mathfrak{L}$ for which $\mathrm{g}_{c}(\ell)_{\omega^{5}}$ is a 37 th power.
(ii) Results for $p=157$. For $p=157$ (exponents of $p$-irregularity 62,110 ), one finds the partial analogous information after 590 distinct primes $\ell \in \mathscr{L}_{p}$ tested (proving also Vandiver's conjecture for a lot of times):

```
Nel Npp el
590 309 1161487 [9,3,2,6,8,3,1,4,5,10,3,1,3,1,6,3,4,4,2,2,1,2,5,
    5,3,2,2,1,5,7,6,2,2,1,5,5,5,4,4,3,3,4,5,4,5,5,5,5,5,3,6,1,6,3,5,4,5,
    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]
```

These numbers may depend on the orders of $\omega^{n}$ and/or $\omega^{p-n}$, but this needs to be clarified taking much $\ell \in \mathscr{L}_{p}$.
4.4.3. Vandiver's conjecture and $\boldsymbol{p}$-adic regulator of $\boldsymbol{K}_{+}$. We return to the case $p=37$ and $n_{0}=32$. 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 $\mathcal{T}_{k_{9}} \neq 1$ from the reflection relation (3.1); so, $k_{9}$ admits a cyclic 37 -ramified extension of degree 37 which is not unramified. To verify, we use [17, Program I], for real fields, which indeed gives $\# \mathcal{T}_{k_{9}}=37$ (nt must verify $\mathrm{p}^{\text {nt }}>p^{t}$, the exponent of $\mathcal{T})$ :

```
{p=37;n=32;d=(p-1)/gcd(p-1,n);P=polsubcyclo(p,d);K=bnfinit(P,1);nt=6;
Kpn=bnrinit(K,p^nt);Hpn=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 $\# \mathcal{T}_{+}=\# C \ell_{+} \cdot \# \mathcal{R}_{+}$, where the $p$-group $\mathcal{R}_{+}$is the normalized $p$-adic regulator of $K_{+}$ [19, Proposition 5.2]. Whence $\# \mathcal{T}_{\chi}=\# \mathcal{C l}_{\chi} \cdot \# \mathcal{R}_{\chi}$ and $\mathcal{R}_{\chi^{*}}=1$, for all $\chi \in \mathscr{X}_{+}$; but we have $\# \mathcal{T}_{\chi^{*}}=\# \widetilde{C}_{\chi_{\chi *}}$ for the subgroup $\widetilde{\mathcal{C}}_{\chi^{*}}$ of $\mathcal{C}_{\chi^{*}}$. The above data shows that the relation $\# \mathcal{T}_{\chi_{0}}=37$ comes from $\# \mathcal{R}_{\chi_{0}}=37$, which is not surprising:
Remark 4.11. We have the analytic formula $\# \mathcal{C l}_{\chi_{0}}=\#\left(E_{\chi_{0}} /\left\langle\eta_{\chi_{0}}\right\rangle\right)$, where $\eta$ is a suitable cyclotomic unit; so a classical method (explained in [52, Corollary 8.19], applied in [4, 9] and developped in $[50,51])$ consists in finding $\ell \in \mathscr{L}_{p}$ 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 $\mathcal{R}_{\chi_{0}} \neq 1$ (with $\mathcal{C}_{\chi_{0}}=1$ ), this means that $\eta_{\chi_{0}}$ generates $E_{\chi_{0}}$ and is a local $p$ th power at $p$ by $p$-primarity, so that $K\left(\sqrt[p]{\eta_{\chi_{0}}}\right)$ is contained in the $\chi_{0}^{*}$-component of the $p$-Hilbert class field of $K$.
We shall give in $\S 5.2 .4$ some insights in this direction to state new heuristics for the probability of $p$-primarity of $\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}}$ to be at most $\frac{O(1)}{p^{2}}$.

## 5. Heuristics - Probability of a counterexample

5.1. Use of classical standard probabilities. We may suppose in a first approximation that, for a given $p$, the sets $\mathscr{E}_{\ell}(p)$ of exponents of $p$-primarity of primes $\ell \in \mathscr{L}_{p}$, are random with the same behavior as for the set $\mathscr{E}_{0}(p)$ of exponents of $p$-irregularity. More precisely, assume, as in Washington's book (see in [52], the Theorem 5.17 and some statistical computations), that for given primes $p$ and $\ell \in \mathscr{L}_{p}$, the probabilities of a cardinality $k$ is $\binom{N}{j} \cdot\left(1-\frac{1}{p}\right)^{N-j} \cdot\left(\frac{1}{p}\right)^{j}\left(\right.$ where $\left.N:=\frac{p-3}{2}\right)$. 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 $\ell$ given, of $\mathscr{E}_{0}(p) \cap \mathscr{E}_{\ell}(p) \neq \emptyset$ with cardinalities $j \in[0, N]$ and $k \in[0, N]$ fixed, is:

$$
1-\frac{(N-k)!\cdot(N-j)!}{N!\cdot(N-k-j)!} .
$$

So, an approximation of the whole probability of $\mathscr{E}_{0}(p) \cap \mathscr{E}_{\ell}(p) \neq \emptyset$ is:

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

The computations show that this expression is around $\frac{1}{2 p}$, which does not allow to conclude easily for a single $\ell$, but this does not take into account the "infiniteness" of $\mathscr{L}_{p}$ giving, a priori, independent informations, but limited by the Theorem 3.7 on periodicities due to the density theorem (see the Weil interpretation of Jacobi sums defining Hecke Grössencharacters [55, Theorem, p. 489] where a module of definition of our Jacobi sums is $p^{2}$, which may give an order of magnitude of the cardinality of this "infiniteness"). So this must be put in relation with the Theorem 4.7 to characterize "non-Vandiver".
5.2. New heuristics and probabilities. Many reasons imply that the generic probability $\frac{1}{p}$ must be replaced by a much lower one:
5.2.1. Results from K-theory. For some characters $\chi \in \mathscr{X}_{+}$, of the form $\chi=: \omega^{p-(1+h)}$, for small $h=2,4, \ldots$, one may prove that $\mathcal{C}_{\omega^{p-(1+h)}}=1$, as the case of $\mathcal{C}_{\omega^{p-3}}=1$ proved unconditionally by Kurihara [30]; then Soulé proved in [48] that for $n \in[2, p-3]$ even, $\mathcal{C}_{\omega^{p-n}}=1$ for all $p$ large enough (see also [11, 49, 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, $\mathcal{C}_{\chi}$ may be trivial because of the "archimedean" order of magnitude of the whole class number of the subfield of $K_{+}$fixed by $\operatorname{Ker}(\chi)$ (which is proved for the quadratic case when $p \equiv 1(\bmod 4)$, the cubic case when $p \equiv 1(\bmod 3)$ ); see the tables of Schoof $[42]$ for serious arguments about the order of magitude of the whole class number. Moreover, we have the $p$-rank $\epsilon$-conjecture for $p$-class groups [10] that we state for the real abelian fields $k_{d}$ of constant degree $d$, of discriminant $D=p^{d-1}$, when $p \equiv 1(\bmod d)$ increases:

For all $\epsilon>0$ there exists $C_{p, \epsilon}$ such that $\log \left(\#\left(\mathcal{C}_{k_{d}} / \mathcal{C} \ell_{k_{d}}^{p}\right)\right) \leq \log \left(C_{p, \epsilon}\right)+\epsilon \cdot \log (p)$,
which would give $\mathcal{C} \ell_{k_{d}}=1$ for $\log (p)>\frac{\log \left(C_{p, \epsilon}\right)}{1-\epsilon}$ and any $\epsilon<1$. But this does not apply for any $p$ with "small" $d$ and the constant $C_{p, \epsilon}$ is not effective.
5.2.3. Heuristics about Gauss sums. The standard probabilities (11) assume that when $\ell \in \mathscr{L}_{p}$ varies, the sets $\mathscr{E}_{\ell}(p)$ are random and independent, giving probabilities close to 0 , which is not the case when $p$ is irregular at some $\chi_{0}^{*}=\omega^{p-n_{0}}$ with $\mathcal{C l}_{\chi_{0}^{*}} \simeq \mathbb{Z} / p^{e} \mathbb{Z}, e \geq 1$, and when $\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}}$ is a global $p$ th power because $\mathfrak{L}_{\chi_{0}^{*}}^{p^{e-1}}$ is $p$-principal.
Fix $\ell \in \mathscr{L}_{p}$ such that $\mathfrak{L}_{\chi_{0}^{*}}$ generates $\mathcal{C}_{\chi_{0}^{*}} \simeq \mathbb{Z} / p^{e} \mathbb{Z}$ (thus $\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}}$ is not a global $p$ th power); put (Proposition 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 $\varpi$ if and only if $\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}}$ is not $p$-primary.
Whatever $\ell^{\prime} \in \mathscr{L}_{p}$ and $\mathfrak{L}^{\prime} \mid \ell^{\prime}$, one has, from $\S 4.3(\mathrm{ii}), \mathrm{g}_{c}\left(\ell^{\prime}\right)_{\chi_{0}^{*}} \equiv \mathrm{~g}_{c}(\ell)_{\chi_{0}^{*}}^{r}(\bmod p)$, with $r \in\left[0, p^{e}-1\right]\left(r=0\right.$ if $\mathfrak{L}_{\chi_{0}^{*}}^{\prime}$ is $p$-principal, thus $\left.\mathrm{g}_{c}\left(\ell^{\prime}\right)_{\chi_{0}^{*}} \in K^{\times p}\right)$, giving:

$$
\begin{equation*}
\mathrm{g}_{c}\left(\ell^{\prime}\right)_{\chi_{0}^{*}}=: 1+\beta_{0}\left(\ell^{\prime}\right) \cdot \varpi^{p-n_{0}}, \beta_{0}\left(\ell^{\prime}\right) \equiv r \cdot \beta_{0}(\ell)(\bmod \varpi) . \tag{12}
\end{equation*}
$$

Contrary to the classical idea that $\beta_{0}(\ell)(\bmod \varpi)$ follow standard probabilities $\frac{O(1)}{p}$ (even under the condition $\left.\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}} \notin K^{\times p}\right)$, we propose the following heuristic:

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

Because of the density theorems on the ideal classes when $\ell$ varies in $\mathscr{L}_{p}$ and $\chi$ in $\mathscr{X}_{+}$, we must examine two cases concerning the $\chi$-components of $\mathcal{C}$ when there exists $\chi_{0}=\omega^{n_{0}} \in \mathscr{X}_{+}$ such that $\mathcal{C}_{\chi_{0}^{*}} \simeq \mathbb{Z} / p^{e} \mathbb{Z}, e \geq 1$ :
(a) $\chi \neq \chi_{0}$ and $\mathcal{C l}_{\chi_{*}}=1$. 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 $\beta(\ell)(\bmod \varpi)\left(\right.$ probabilities $\left.\frac{O(1)}{p}\right)$.
(b) $\chi=\chi_{0}$ (and $\mathcal{C}_{\chi_{0}^{*}} \neq 1$ ). If $\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}}$ is $p$-primary for some given generator $\mathfrak{L}_{\chi_{0}^{*}}$, then from (12) all the $\mathrm{g}_{c}\left(\ell^{\prime}\right)_{\chi_{0}^{*}}$ are $p$-primary, whatever the class of $\mathfrak{L}_{\chi_{0}^{*}}^{\prime}$ ( $p^{e}$ possibilities) because $\beta_{0}\left(\ell^{\prime}\right) \equiv 0(\bmod \varpi)$. So, $n_{0}$ is always in $\mathscr{E}_{\ell}(p)$ and $\mathscr{E}_{0}(p) \cap \mathscr{E}_{\ell}(p) \neq \emptyset$ for all $\ell \in \mathscr{L}_{p}$, which corresponds to $\mathcal{C} \chi_{\chi_{0}} \neq 1$ and the non-cyclicity of $\mathcal{C l}_{\chi_{0}^{*}}^{(p)}$ (Theorem 3.7).
Thus, to have analogous densities of $p$-primarity on $\mathscr{L}_{p}$ (as for the $p$-principal case (a)), $\beta_{0}(\ell) \equiv 0(\bmod \varpi)$ (under the condition $\left.\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}} \notin K^{\times p}\right)$ must occur at least $p$ times less,
giving a probability in $\frac{O(1)}{p^{2}}$ instead of $\frac{O(1)}{p}$; it is even possible that such a circumstance be of probability 0 depending on more accurate properties of Gauss or Jacobi sums; for this, the computation of $\beta(\ell)$ should be very interesting (see [51] where, for any $\ell \equiv 1(\bmod p)$, the coefficients $d_{i, k}$ of $J_{i}:=\sum_{k=0}^{p-1} d_{i, k} \zeta_{p}^{k}$, with $\sum_{k=0}^{p-1} d_{i, k}=1$, are studied and the starting point of future investigations, in relation with the other heuristics).
5.2.4. Use of $\boldsymbol{p t h}$ power residue symbols and cyclotomic units. We refer to [52, $\oint 8.3]$ for the classical $p$-adic interpretation of the numbers $\# C l_{\chi}$, for $\chi \in \mathscr{X}_{+}$, as indices of the form $\left(E_{\chi}: F_{\chi}\right)$, where $F$ is the group of cyclotomic units.
We need the following $p$ th power criterion (from [15, II.6.3.8]):
Lemma 5.1. Let $\alpha \in K^{\times}$be a pseudo-unit (namely, $\alpha$ is prime to $p$ and $(\alpha)=\mathfrak{a}^{p}$ ). Let any set $\mathscr{S}$ of places $\mathfrak{q}$ of $K$ such that $\langle c l(\mathscr{S})\rangle_{\mathbb{Z}}=\mathcal{C l}$ (or such that $\langle c l(\mathscr{S})\rangle_{\mathbb{Z}[G]}=\mathcal{C l}$ if $K(\sqrt[p]{\alpha}) / \mathbb{Q}$ is Galois).
Then $\alpha \in K^{\times p}$ if and only if $\alpha$ is p-primary and locally a pth power at $\mathscr{S}$ (i.e., $\alpha \in K_{\mathfrak{q}}^{\times p}$ for all $\mathfrak{q} \in \mathscr{S}$ where $K_{\mathfrak{q}}$ is the $\mathfrak{q}$-completion of $K$ ).

Proof. Consider the non-trivial direction, in the Galois case, assuming that $\alpha$ is $p$-primary and such that $\alpha \in K_{\mathfrak{q}}^{\times p}$ for all $\mathfrak{q} \in \mathscr{S}$. So $K(\sqrt[p]{\alpha}) / K$ is unramified and $\mathscr{S}$-split; thus, due to the Galois condition, all the conjugates of $\mathfrak{q} \in \mathscr{S}$ split and the Galois group of $K(\sqrt[p]{\alpha}) / K$ corresponds, by class field theory, to a quotient of $\mathcal{C l} /\langle C l(\mathscr{S})\rangle_{\mathbb{Z}[G]}$, trivial by assumption.
Theorem 5.2. Let $\chi_{0}=\omega^{n_{0}} \in \mathscr{X}_{+}$with $n_{0} \in \mathscr{E}_{0}(p)$ and $\mathcal{C} l_{\chi_{0}^{*}} \simeq \mathbb{Z} / p^{e} \mathbb{Z}$, e $\geq 1$ (i.e., $\left.b_{c}\left(\chi_{0}^{*}\right) \sim p^{e}\right)$. Let $\eta:=\zeta_{p}^{\frac{1-c}{2}} \frac{1-\zeta_{p}^{c}}{1-\zeta_{p}}$ be a generating real cyclotomic unit, where $c$ is a primitive root modulo $p$ (cf. [52, Proposition 8.11]).
(i) There exists an infinite subset $\mathscr{L}_{p}\left(\chi_{0}\right) \subseteq \mathscr{L}_{p}$ of primes $\ell$ such that the G-module generated by the p-class of $\mathfrak{L} \mid \ell$ is $\mathcal{C l}_{\chi_{0}} \oplus \mathcal{C l}_{\chi_{0}^{*}}$.
(ii) $\mathcal{C l}_{\chi_{0}} \neq 1$ if and only if $\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}}$ is locally a pth power at $\mathfrak{p}$ but not at $\mathfrak{L}\left(\ell \in \mathscr{L}_{p}\left(\chi_{0}\right)\right)$.
(iii) $\mathcal{C} \ell_{\chi_{0}} \neq 1$ if and only if $\eta_{\chi_{0}}$ is locally a pth power at $\mathfrak{p}$ and at $\mathfrak{L}\left(\ell \in \mathscr{L}_{p}\left(\chi_{0}\right)\right)$.

Proof. (i) In the $\mathbb{Z}_{p}[G]$-monogenous case, the ideals $\mathfrak{L}$ are of the form $(z) \cdot \mathfrak{A} \cdot \mathfrak{A}^{*}, z \in K^{\times}$, where $d(\mathfrak{A})$ generates $\mathcal{C} \ell_{\chi_{0}}$ and $d\left(\mathfrak{A}^{*}\right)$ generates $\mathcal{C} \chi_{\chi_{0}^{*} .}{ }^{2}$
(ii) $\&$ (iii) Define the $p$ th power residue symbol $\left(\frac{\alpha}{\mathfrak{L}}\right):=\alpha^{\frac{\ell-1}{p}}(\bmod \mathfrak{L})$ for $\mathfrak{L} \mid \ell \in \mathscr{L}_{p}$ when $\alpha \in K^{\times}$is prime to $\mathfrak{L}$. By abuse of notation, we shall write $\left(\frac{\alpha}{p}\right)=1$ if $\alpha$ is $p$-primary and $\left(\frac{\alpha}{\mathfrak{L}}\right)=1$ if $\alpha \in K_{\mathfrak{L}}^{\times p}$ is not prime to $\mathfrak{L}$. Take $\ell \in \mathscr{L}_{p}\left(\chi_{0}\right)$ :
(a) Consider $\alpha=\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}}$, where $\left(\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}}\right)=\mathfrak{L}_{\chi_{0}^{*}}^{b_{c}\left(\chi_{0}^{*}\right)}$. This gives rise to a counterexample to Vandiver's conjecture at $\chi_{0}$ if and only if $\alpha$ is $p$-primary since $c \ell\left(\mathfrak{L}_{\chi_{0}^{*}}\right)$ is a generator of $\mathcal{C l}_{\chi_{0}^{*}}$; it follows that $\left(\frac{\alpha}{\mathfrak{L}}\right) \neq 1$, otherwise, from Lemma 5.1 applied in $H_{\chi_{0}}, \alpha=\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}}$ should be a global $p$ th power (contradiction).

[^2] and $\mathcal{C}_{\chi_{0}^{*}} \simeq \mathbb{Z} / p \mathbb{Z}$, the density is $1-\frac{1}{p}$.
(b) Consider $\alpha=\eta_{\chi_{0}}$. Thus $b_{c}\left(\chi_{0}^{*}\right) \equiv 0(\bmod p)$ is equivalent to the $p$-primarity of $\eta_{\chi_{0}}$; so a counterexample to Vandiver's conjecture at $\chi_{0}$, equivalent to $\eta_{\chi_{0}} \in E_{\chi_{0}}^{p}$, is equivalent to $\left(\frac{\eta_{\chi_{0}}}{\mathfrak{L}}\right)=1$ since $\left(\frac{\eta_{\chi_{0}}}{p}\right)=1$. Whence, with a prime $\mathfrak{L} \mid \ell \in \mathscr{L}_{p}\left(\chi_{0}\right)$ :
$$
\mathcal{C}_{\chi_{0}} \neq 1 \Leftrightarrow\left(\frac{\mathrm{~g}_{c}(\ell)_{\chi_{0}^{*}}}{\mathfrak{L}}\right) \neq 1 \&\left(\frac{\mathrm{~g}_{c}(\ell)_{\chi_{0}^{*}}}{p}\right)=1 \Leftrightarrow\left(\frac{\eta_{\chi_{0}}}{\mathfrak{L}}\right)=\left(\frac{\eta_{\chi_{0}}}{p}\right)=1 .
$$

Let $\chi \in \mathscr{X}_{+}$and $\ell \in \mathscr{L}_{p}(\chi)$ fixed. If $\operatorname{Prob}\left(\left(\frac{\mathrm{g}_{c}(\ell)_{\chi^{*}}}{\mathcal{L}^{\prime}}\right) \neq 1\right)$ is close to 1 , this suggests a probability around $\frac{O(1)}{p^{2}}$ for the $p$-primarity of $\mathrm{g}_{c}(\ell)_{\chi^{*}}$ if the two above symbols of $\eta_{\chi}$ are independent with probabilities $\frac{O(1)}{p}$ for a single $\ell$.
So it is necessary to compute the symbol $\left(\frac{\mathrm{g}_{c}(\ell)_{0}^{*}}{\mathfrak{L}}\right)$ since $\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}}$ and $\mathfrak{L}$ are non-independent data. For $\chi_{0}=\omega^{n_{0}}, n_{0} \in \mathscr{E}_{0}(p)$, the primes $\ell$ of the theorem are not effective, but experiments with random $\ell$ seem sufficient for statistics. Then a first condition for $\left(\frac{\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}}}{\mathcal{L}}\right)=1$ is that $\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}}$ be the $p$ th power of an $\ell$-ideal, which is fulfilled since $b_{c}\left(\chi_{0}^{*}\right) \equiv 0(\bmod p)$.
Then, using the general program computing $\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}}$ in $\mathrm{Sn} \in \mathbb{Z}\left[\zeta_{p}\right]$ (in other words not reduced modulo $p$ ), we divide this integer by the maximal power $\ell^{v}$, so that there exists a prime ideal $\mathfrak{L} \mid \ell$ which does not divide this new integer (still denoted $S n$ and $p$ th power of an $\ell$-ideal); the computation reduces to $R$, prime to $\mathfrak{L}$ and most likely random, whose symbol $\left(\frac{R}{\mathfrak{L}}\right)=R^{\frac{\ell-1}{p}}$ $(\bmod \mathfrak{L})$, computed in $u$, is immediate and gives the statistics:

```
{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!=0,print("Sn GLOBAL pth power")))}
p=37 n=32
el=149 v=259 u=102 Sn NON local pth power at L
el=223 v=259 u=132 Sn NON local pth power at L
el=6883 v=259 u=6850 Sn NON local pth power at L
el=7253 v=259 u=4947 Sn NON local pth power at L
el=32783 v=259 u=1 Sn local pth power at P
el=32783 v=259 u=1 Sn local pth power at L
el=32783 v=259 u=1 Sn GLOBAL pth power
```

We found $u=\left(\frac{\mathrm{g}_{c}(\ell)_{0}^{*}}{\mathfrak{L}}\right)=1$ for the following $\ell$ (including the underlined numbers corresponding to primes $\ell \notin \mathscr{L}_{p}\left(\chi_{0}\right)$ such that $\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}} \in K^{\times p}$, i.e., $\mathcal{L} p$-principal):
$\ell \in\{22571 ; 32783 ; 46103 ; 53503 ; 57943 ; 64381 ; 67489 ; 68821 ; 79847 ; 83177 ; 96497 ; 98939 ; 104933 ; 108929 ;$
$117883 ; \underline{132313} ; 146521 ; \underline{146891} ; 151553 ; 151849 ; 158657 ; 158731 ; 167759 ; 172717 ; 197359 ; 198839, \underline{207497}\}$
confirming existence and rarity of primes $\ell$ in the interval [149; 207497] such that $u=1$ by $\operatorname{accident}\left(\mathrm{g}_{c}(\ell)_{\chi_{0}^{*}} \notin K^{\times p}\right.$, i.e., $\mathcal{L}$ non- $p$-principal).
For $n=22 \notin \mathscr{E}_{0}(37)$, we found $u=1$ for the few examples (up to $2 \cdot 10^{5}$ ):
$\ell \in\{2221 ; 2887 ; 3923 ; 49211 ; 51283 ; 69709 ; 147779 ; 164503 ; 170497 ; 179969 ; 192697 ; 197803\}$
but $\mathrm{g}_{c}(\ell)_{\chi^{*}}$ is not the $p$ th power of an $\ell$-ideal, whence it is never in $K_{\mathfrak{L}}^{\times p}$. One finds an exponent of $p$-primarity 22 for $\ell=3331$, then 14,16 for $\ell=51283$, 10 for $\ell=147779$, and 28 for $\ell=164503$. In the exceptional case $\ell=3331, \mathrm{~g}_{c}(\ell)_{\chi^{*}}$ is $p$-primary.
This confirms the expected properties of the symbol $\left(\frac{g_{c}\left(\ell \chi_{0}^{*}\right.}{\mathcal{L}}\right)$. A similar program computing the two symbols of $\eta_{\chi_{0}}$ gives all expected results.
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 $C \ell_{\chi *}^{(p)}$ when it is, for instance, of order $p^{2}$.
Whatever the (numerous) references concerning this subject and independently of some improvements or questions on the relevance of the formulas giving $\operatorname{Prob}\left(\mathrm{rk}_{p}(C)=r\right)$ for such a $p$-group $C$, we observe that the quotient of the two probabilities for $r=2$ and $r=1$ (for instance under the condition $\# C=p^{2}$ ) is at most $\frac{O(1)}{p}$ giving probabilities in $\frac{O(1)}{p^{2}}$ to have $\mathcal{C} \ell_{\chi *}^{(p)} \simeq(\mathbb{Z} / p \mathbb{Z})^{2}$. Since $\mathrm{rk}_{p}\left(\mathcal{C l}_{\chi}\right)=1$ splits in the two cases of the reflection theorem, $\mathrm{rk}_{p}\left(\mathcal{C l}_{\chi} \oplus \mathcal{C l}_{\chi^{*}}\right)=2$ or $\mathrm{rk}_{p}\left(\mathcal{C l}_{\chi^{*}}\right)=2$, the above applies. As Nguyen Quang Do pointed out, this may come from the relation $\mathrm{H}^{2}\left(\mathcal{C l}_{\chi^{*}},(V / W)_{\chi^{*}}\right) \simeq \mathbb{F}_{p}$, assuming the uniform randomness of the exact sequences $1 \rightarrow(V / W)_{\chi^{*}} \simeq \mathbb{F}_{p} \rightarrow \mathcal{C l}_{\chi^{*}}^{(p)} \rightarrow \mathcal{C l}_{\chi^{*}} \simeq \mathbb{F}_{p} \rightarrow 1$ (proof of Theorem 3.7), the non-cyclic case corresponding to the single cohomology class 0 .
5.2.6. Heuristics from $p$-ramification theory. Another investigation is about the groups $\mathcal{T}_{\chi}, \chi \in \mathscr{X}_{+}$, and the formula $\# \mathcal{T}_{\chi}=\# \mathcal{C l}_{\chi} \cdot \# \mathcal{R}_{\chi}$ with the equivalence (3.1) of reflection, $\mathcal{C l}_{\chi^{*}} \neq 1$ if and only if $\mathcal{T}_{\chi} \neq 1$ (illustrated in §4.4.3).
Indeed, it is interesting to estimate in what proportions the relation $\# \boldsymbol{C l}_{\chi} \cdot \# \mathcal{R}_{\chi} \neq 1$ 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 [20] and its bibliography), we give some examples with quadratic and cyclic cubic fields.
(a) Real quadratic fields and $p \geq 3$ fixed. For each of the ND real quadratic field of discriminant $\mathrm{D} \in[\mathrm{bD}, \mathrm{BD}]$, for which $\mathcal{T} \neq 1$ (counted in Nt ), we compute the proportions of cases for which this is due to $\# \mathcal{C l}$ or $\# \mathcal{R}$; we privilegiate the case $\mathcal{C l} \neq 1$ (counted in Nh ) even if the two groups $\mathcal{C l}$ and $\mathcal{R}$ are both non-trivial; this may give a slightly larger proportion for $\frac{\mathrm{Nh}}{\mathrm{Nt}}$ but a much faster program:

```
{p=3;bD=10^6;BD=10^6+5*10^4;ND=0;Nh=0 ; Nt=0; for(D=bD,BD,e=valuation(D , 2) ; M=D/2^e ;
if(core(M)!=M,next);if((e==1||e>3)||(e==0&Mod(M,4)!=1)||(e==2&Mod(M,4)==1),next);
m=D;if(e!=0,m=D/4);ND=ND+1;P=x^2-m;K=bnfinit(P,1);Kpn=bnrinit(K,p^2);
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+O.," 1/p=",1./p)}
[bD, BD]=[1000000, 1050000]
p=3 ND=15204 Nt=7308 Nh=2050 Nh/Nt=0.28051450 1/p=0.33333333
p=5 ND=15204 Nt=3522 Nh=634 Nh/Nt=0.18001135 1/p=0.20000000
p=7 ND=15204 Nt=2464 Nh=331 Nh/Nt=0.13433441 1/p=0.14285714
p=11 ND=15204 Nt=1497 Nh=97 Nh/Nt=0.06479625 1/p=0.09090909
```

$[b D, B D]=[10000000,10050000]$

```
\begin{tabular}{llllll}
\(p=3\) & \(N D=15198\) & \(\mathrm{Nt}=7516\) & \(\mathrm{Nh}=2161\) & \(\mathrm{Nh} / \mathrm{Nt}=0.28751995\) & \(1 / \mathrm{p}=0.33333333\) \\
\(\mathrm{p}=5\) & \(\mathrm{ND}=15198\) & \(\mathrm{Nt}=3597\) & \(\mathrm{Nh}=720\) & \(\mathrm{Nh} / \mathrm{Nt}=0.20016680\) & \(1 / \mathrm{p}=0.20000000\) \\
\(\mathrm{p}=7\) & \(\mathrm{ND}=15198\) & \(\mathrm{Nt}=2443\) & \(\mathrm{Nh}=347\) & \(\mathrm{Nh} / \mathrm{Nt}=0.14203847\) & \(1 / \mathrm{p}=0.14285714\) \\
\(\mathrm{p}=11\) & \(\mathrm{ND}=15198\) & \(\mathrm{Nt}=1512\) & \(\mathrm{Nh}=122\) & \(\mathrm{Nh} / \mathrm{Nt}=0.08068783\) & \(1 / \mathrm{p}=0.09090909\)
\end{tabular}
[bD, BD] = [100000000, 100100000]
p=3 N=30410 Nt=15133 Nh=4456 Nh/Nt=0.29445582 1/p=0.33333333
```

The proportion $\mathrm{Nh} / \mathrm{Nt}$ becomes close to $\frac{1}{p}$ for intervals with large discriminants.
(b) Cyclic cubic fields and $p \equiv 1(\bmod 3)$ fixed. We obtain analogous results with the same rough calculation (e.g., we may have $\mathcal{C} \chi_{\chi_{1}} \neq 1$ and $\mathcal{R}_{\chi_{1}} \neq 1$ or $\mathcal{R}_{\chi_{2}} \neq 1$ ), but this does not affect the statistics ( $\mathrm{f} \in[\mathrm{bf}, \mathrm{Bf}]$ 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
```

The fact that $\mathcal{R}_{\chi}$ is much often non-trivial than $\mathcal{C l}_{\chi}$, in a computable proportion, is a positive argument for Vandiver's conjecture. We suggest that for totally real fields (like $K_{+}$), abelian $p$-ramification is essentially governed by the normalized $p$-adic regulator and that the $p$-class group is in some sense a "secondary" invariant.
5.2.7. Folk heuristic. Consider the Gauss $\operatorname{sum} \tau(\psi)=-\sum_{k=0}^{\ell-2} \zeta_{p}^{k} \cdot \xi_{\ell}^{g^{k}}$ (where $g$ is a primitive root modulo $\ell, \zeta_{p}:=\psi(g)$, see (6)), and put $k=a p+b, 0 \leq a \leq \frac{\ell-1}{p}-1,0 \leq b \leq p-1$. Whence:

$$
\begin{equation*}
\tau(\psi)=-\sum_{b=0}^{p-1} \zeta_{p}^{b} \cdot\left[\operatorname{Tr}_{\mathbb{Q}\left(\xi_{\ell}\right) / F_{\ell}}\left(\xi_{\ell}\right)\right]^{\sigma(b)} \tag{13}
\end{equation*}
$$

where $F_{\ell}$ is the cyclic subextension of degree $p$ of $\mathbb{Q}\left(\xi_{\ell}\right)$, where $\sigma(b)$ is the automorphism acting trivially on $\zeta_{p}$ and such that $\xi_{\ell} \mapsto \xi_{\ell}^{g^{b}}$, giving an exact system of representatives for $\operatorname{Gal}\left(F_{\ell} / \mathbb{Q}\right)$ independent of the choice of $g$.
From Remark 3.5 (ii), we know that $F_{\ell}$ is obtained as the decomposition over $\mathbb{Q}$ of the extension $K(\sqrt[p]{\alpha}) / K$, with $\alpha=\tau(\psi)^{p} \in \mathbb{Z}\left[\zeta_{p}\right]$, and it is immediate to see that the $p$-class group of
$F_{\ell}$ is trivial because of Chevalley's formula on invariant classes giving here $\# C_{F_{\ell}}^{\mathrm{Gal}\left(F_{\ell} / \mathbb{Q}\right)}=1$ since $\ell$ is the unique ramified prime in $F_{\ell} / \mathbb{Q}$.
(i) The first observation is that the $p$-class group of $F_{\ell}$ does not depend on that of $K$ as $\ell$ varies! Indeed, this context is neither more nor less than class field theory over $\mathbb{Q}$ giving the existence of a unique cyclic extension $F_{\ell}$ of conductor $\ell \equiv 1(\bmod p)$, for which one considers the set of conjugates of the relative trace of $\xi_{\ell}$ which moreover defines a normal basis of $F_{\ell}$; then the unique link with the arithmetic of $K$ is the linear combination (13) involving the traces to built $\alpha$, but the character of $\langle\alpha\rangle_{\mathbb{Z}[G]} K^{\times p} / K^{\times p}$ is $\omega$ which gives, as we know, a "poor" information on the arithmetic of $K$.
Thus, the relationship of $\alpha=\tau(\psi)^{p}$ (whence of $\tau(\psi)$ ) with class field theory over $K$ (namely, with $p$-classes and units of $K$ ) is tenuous, possibly empty; which is quite the opposite for the twists $\mathrm{g}_{c}(\ell)$ because of the relations $\alpha^{c-s_{c}}=\mathrm{g}_{c}(\ell)^{p}$ and the fact that the $\mathrm{g}_{c}(\ell)_{\chi^{*}}$ are radicals defining non-trivial (arithmetically) cyclic extensions of degree $p$ of $K_{+}$for any even character $\chi$.
(ii) In another direction, suggested by the work of Lecouturier [33] generalizing results of Calegari-Emerton and Iimura, 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 $\ell \not \equiv 1\left(\bmod p^{2}\right)$. On the contrary, as shown by many results of [33], 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 $\widetilde{M}:=K(\sqrt[p]{\widetilde{\alpha}})$ :

$$
\# C C_{\widetilde{M}}^{\operatorname{Gal}(\widetilde{M} / K)}=\# \mathcal{C} \ell_{K} \cdot \frac{p^{p-2+\delta}}{\left(E_{K}: E_{K} \cap \mathrm{~N}_{\widetilde{M} / K}\left(\widetilde{M}^{\times}\right)\right)} \leq \# \mathcal{C l}_{K} \cdot p^{\frac{p-1}{2}}
$$

where $\delta=1$ or 0 according as $p$ ramifies or not and where $\zeta_{p}$ is norm for $\delta=0$; but the non-abelian Galois structure yields various non-trivial p-class groups for $\widetilde{F}_{\ell}$ as $\ell$ varies, and genera theory implies $\mathrm{rk}_{p}\left(\mathcal{C l}_{\tilde{F}_{\ell}}\right) \geq 1$ for all $\ell$ (for the metabelian genera theory, see [29]). However, for $M=K(\sqrt[p]{\alpha})=F_{\ell} K$ :

$$
\# \mathcal{C l}_{M}^{\mathrm{Gal}(M / K)}=\# \mathcal{C l}_{K} \cdot \frac{p^{p-2}}{\left(E_{K}: E_{K} \cap \mathrm{~N}_{M / K}\left(M^{\times}\right)\right)} \leq \# \mathcal{C l}_{K} \cdot p^{\frac{p-1}{2}}
$$

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

Because of $F_{\ell}$ defined by the radical $\alpha=\tau(\psi)^{p}$, the p-adic properties of the Gauss sums are independent of the arithmetic of $K$ as $\ell$ varies (despite the apparent complexity of the radical $\left.\alpha=\tau(\psi)^{p}\right)$, 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 $\chi^{*}$-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 $\ell$ varies, and this probably has an impact on the multiplicative properties regarding the results of $\S 4.3$. We shall examine the case of the twists $\mathrm{g}_{c}(\ell)$ (more precisely
of $\left.\psi^{-c}(c) \mathrm{g}_{c}(\ell)\right)$, then the case of the original Gauss sums $\tau(\psi)$ from the arithmetic of the fields $F_{\ell}$.
5.3.1. $\mathbb{Z}$-rank of the family $\left(\psi^{-c}(c) g_{c}(\ell)\right)_{\ell \in \mathscr{L}_{p}}$. Put, for $p$ and $c$ fixed:

$$
\begin{equation*}
\mathbf{J}(\ell):=\psi^{-c}(c) \mathrm{g}_{c}(\ell)=\psi^{-c}(c) \tau(\psi)^{c-\sigma_{c}}=J_{1} \cdots J_{c-1}(\text { see }(10)) \tag{14}
\end{equation*}
$$

written on the basis $\left\{1, \zeta_{p}, \ldots, \zeta_{p}^{p-2}\right\}$, under the form $\mathbf{J}(\ell)=\sum_{k=0}^{p-2} a_{k}(\ell) \zeta_{p}^{k}$, the integers $a_{k}(\ell)$ being considered modulo $p$. A first information, about the $p$-adic repartition of the $\mathbf{J}(\ell)$ as $\ell$ varies, is to compute the $\mathbb{F}_{p}$-rank of the $\mathbb{F}_{p}$-matrix $\left(a_{k}(\ell)\right)_{k, \ell}$. The following program gives systematically:

$$
\operatorname{Rank}_{\mathbb{F}_{p}}\left[\left(a_{k}(\ell)\right)_{\ell, k}\right]=p-4,
$$

for all the primes $p \geq 7$ tested (rank 1 for $p=3$ and rank 2 for $p=5$ ), despite the fact that the lines are not canonical (up to circular permutations of their elements since $\mathbf{J}(\ell)$ is defined up to conjugation). We have verified it up to $p \leq 331$, an interval which contains 16 irregular primes. The program gives $p$, the $\mathbb{F}_{p}$-rank of the matrix (in rank) and the least $\ell_{p}$ (in elp) for which the sub-matrix built from $\left\{\ell \in \mathscr{L}_{p}, \ell \leq \ell_{p}\right\}$ has rank $p-4$ :

| \{forprime( $\mathrm{p}=7,500, \mathrm{c}=\operatorname{lift}(\operatorname{znprimroot(p));P=polcyclo(p)+Mod(0,p);M=matrix(0,p-1)}$ $r=0$; for (i=1,10^8,el=1+2*i*p;if(isprime(el)!=1,next); g=znprimroot(el);J=1; |  |  |  |  |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| $A=$ concat ( $M, V$ ) ; rr=matrank (A) ;if (rr==r, next) ; $r=r r$; M $=$ A; |  |  |  |  |  |  |  |  |  |
| if (r==p-4,print("p=",p," r=",r," elp=",el);break)) ) |  |  |  |  |  |  |  |  |  |
| $p$ rank elp | p | rank | elp | p | rank | elp | p | rank | elp |
| 73113 | 11 | 7 | 397 | 13 | $\bigcirc$ | 599 | 17 | 13 | 1259 |
| (...) |  |  |  |  |  |  |  |  |  |
| $\begin{array}{llll}71 & 67 & 42743\end{array}$ | 73 | 69 | 48473 | 79 | 75 | 50087 | 83 | 79 | 65239 |
| 151147247943 | 157 | 153 | 273181 | 163 | 159 | 294053 | 167 | 163 | 305611 |

We have $\mathbf{J}(\ell) \equiv 1(\bmod \mathfrak{p})$, in other words $\sum_{k=0}^{p-2} a_{k}(\ell) \equiv 1(\bmod p)$, and we can write $\mathbf{J}(\ell)=1+\sum_{k=1}^{p-2} a_{k}(\ell)\left(\zeta_{p}^{k}-1\right)$ depending on $p-2$ parameters; then, due to the relations $\mathbf{J}(\ell)^{1+s_{-1}} \equiv 1(\bmod p)$ and $\mathbf{J}(\ell)^{e_{\omega}} \in K^{\times p}\left(\right.$ because $\left.\omega\left(c-s_{c}\right) \equiv 0(\bmod p)\right)$, this yields the three relations of "derivation" (for $p \geq 7) \sum_{k=1}^{p-2} k^{\delta} \cdot a_{k}(\ell) \equiv 0(\bmod p), \delta \in\{1,2,4\}$, for any $\ell \in \mathscr{L}_{p}$. Whence a $\mathbb{F}_{p}$-rank at most $p-4$, but we have no proof of the equality.
The order of magnitude of $\ell_{p}$ seems to be $O(1) p^{2} \log \left(p^{2}\right)$, which is in agreement with a "conductor" $p^{2}$ for these Hecke Grössencharacters [55, Theorem, p. 489], but the program slows down very much, as $p$ increases, to be more accurate.
Moreover, the number of consecutive primes $\ell$ needed to reach the rank $p-4$ is equal to $p-4$, except probably for finitely many cases, which confirms the above order. Give now the end of the above table with an estimation of the $O(1)$ :

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

The $\mathbb{F}_{p}$-rank $r_{p}(\ell)$ of the $p-1$ conjugates of $\mathbf{J}(\ell)(\bmod p), \ell \in \mathscr{L}_{p}$, is close to $p-4$ (e.g., for $p=37, r_{37}(\ell) \in\{33,32,31,30\}$ in similar proportions, and we only have the local minimum $\left(r_{37}(\ell), \ell\right)=(29,2591)$ for $\ell$ up to 37000 .
5.3.2. Repartition of the conjugates of the traces $\operatorname{Tr}_{\mathbb{Q}\left(\xi_{\ell}\right) / F_{\ell}}\left(\xi_{\ell}\right)$. Let $Z_{F_{\ell}}$ be the ring of integers of $F_{\ell}$ 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 (13) giving $\tau(\psi)=-\sum_{b=0}^{p-1} \zeta_{p}^{b} \cdot\left[\operatorname{Tr}_{\mathscr{Q}\left(\xi_{\ell}\right) / F_{\ell}}\left(\xi_{\ell}\right)\right]^{\sigma(b)}$, the images in $Z_{F_{\ell}} / p Z_{F_{\ell}}$ of the conjugates of the relative traces $\operatorname{Tr}\left(\xi_{\ell}\right):=\operatorname{Tr}_{\mathbb{Q}}\left(\xi_{\ell}\right) / F_{\ell}\left(\xi_{\ell}\right)$ may be easily analysed and compared, for $\ell \in \mathscr{L}_{p}$, by means of the image $R_{\ell}$ in $\mathbb{F}_{p}[x]$ of the polynomial $Q_{\ell}=\prod_{\bar{\sigma} \in \operatorname{Gal}\left(F_{\ell} / \mathbb{Q}\right)}\left(x-\operatorname{Tr}\left(\xi_{\ell}\right)^{\bar{\sigma}}\right) \in \mathbb{Z}[x]$.

Proposition 5.3. Let $\ell_{1}, \ell_{2} \in \mathscr{L}_{p}$ and let $\tau\left(\psi_{1}\right), \tau\left(\psi_{2}\right)$ be the corresponding Gauss sums normalized via $\psi_{1}\left(g_{1}\right)=\psi_{2}\left(g_{2}\right)=\zeta_{p}$. Let $F=F_{\ell_{1}} F_{\ell_{2}}$. If $R_{\ell_{1}} \neq R_{\ell_{2}}$, then for all $\sigma \in \operatorname{Gal}(F K / \mathbb{Q}), \tau\left(\psi_{2}\right) \not \equiv \tau\left(\psi_{1}\right)^{\sigma}\left(\bmod \mathfrak{p}^{p} Z_{F K}\right)$.
Proof. Suppose there exists $\sigma \in \operatorname{Gal}(F K / \mathbb{Q})$ such that $\tau\left(\psi_{2}\right) \equiv \tau\left(\psi_{1}\right)^{\sigma}\left(\bmod \mathfrak{p}^{p} Z_{F K}\right)$; recall that $\tau\left(\psi_{1}\right)^{\sigma}=\zeta_{\sigma} \tau\left(\psi_{1}^{e}\right), \zeta_{\sigma} \in \mu_{p}, e \in(\mathbb{Z} / p \mathbb{Z})^{\times}$. Then:
$\tau\left(\psi_{2}\right)=-\sum_{b=0}^{p-1} \zeta_{p}^{b} \cdot \operatorname{Tr}\left(\xi_{\ell_{2}}\right)^{\sigma_{2}(b)}$ and $\tau\left(\psi_{1}\right)^{\sigma}=-\sum_{b=0}^{p-1} \zeta_{p}^{b} \cdot \operatorname{Tr}\left(\xi_{\ell_{1}}\right)^{\pi\left(\sigma_{1}(b)\right)}$,
where $\pi$ is a permutation of the $\sigma_{1}(b)$. Using $\operatorname{Tr}_{\mathbb{Q}\left(\xi_{\ell_{i}}\right) / \mathbb{Q}}\left(\xi_{\ell_{i}}\right)=-1$, we get:
$\tau\left(\psi_{2}\right)=1-\sum_{b=1}^{p-1}\left(\zeta_{p}^{b}-1\right) \cdot \operatorname{Tr}\left(\xi_{\ell_{2}}\right)^{\sigma_{2}(b)}, \tau\left(\psi_{1}\right)^{\sigma}=1-\sum_{b=1}^{p-1}\left(\zeta_{p}^{b}-1\right) \cdot \operatorname{Tr}\left(\xi_{\ell_{1}}\right)^{\pi\left(\sigma_{1}(b)\right)}$, whence:
$\tau\left(\psi_{1}\right)^{\sigma}-\tau\left(\psi_{2}\right)=\sum_{b=1}^{p-1}\left(\zeta_{p}^{b}-1\right) \cdot\left(\operatorname{Tr}\left(\xi_{\ell_{2}}\right)^{\sigma_{2}(b)}-\operatorname{Tr}\left(\xi_{\ell_{1}}\right)^{\pi\left(\sigma_{1}(b)\right)}\right) \equiv 0\left(\bmod \mathfrak{p}^{p} Z_{F K}\right)$.
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 $\mathfrak{p} Z_{F K}$, this relation implies $\operatorname{Tr}\left(\xi_{\ell_{2}}\right)^{\sigma(b)} \equiv \operatorname{Tr}\left(\xi_{\ell_{1}}\right)^{\pi^{\prime}(\sigma(b))}(\bmod p)$ for all $b$, which yields $R_{\ell_{1}}=R_{\ell_{2}}$ in $\mathbb{F}_{p}[x]$ (contradiction).

Since $\tau\left(\psi_{2}\right) \not \equiv \tau\left(\psi_{1}\right)^{\sigma}\left(\bmod \mathfrak{p}^{p}\right)$ for all $\sigma$ implies $\mathrm{g}_{c}\left(\ell_{2}\right) \not \equiv \mathrm{g}_{c}\left(\ell_{2}\right)^{\sigma}\left(\bmod \mathfrak{p}^{p}\right)$ for all $\sigma$ (except for the $\omega$-components because $\left.\omega\left(c-\sigma_{c}\right) \equiv 0(\bmod p)\right)$, we can say that the number of distinct polynomials $R_{\ell}, \ell \in \mathscr{L}_{p}$, gives a partial idea of the repartition modulo $p$ of the sets $\mathscr{E}_{\ell}(p)$ as $\ell$ varies. As $p$ increases, the number of distinct $R_{\ell}$ seems to be $O\left(p^{2} \cdot \log \left(p^{2}\right)\right)$.
The following program, computing the monic polynomial $\mathrm{R}=R_{\ell} \in \mathbb{F}_{p}[x]$ returns: el $=\ell$, the residue degree $\mathrm{f}=f$ of $p$ in $F_{\ell} / \mathbb{Q}$, and R .

```
{p=7;B=5*10^3;el=1;while(el<B,el=el+2*p;if(isprime(el)!=1,next);g=znprimroot(el);
h=g^p;g=lift(g);h=lift(h);P=polcyclo(el); z=Mod(x,P);Q=1;e=1;for(k=1,p,Tr=0;e=e*g;
for(j=1, (el-1)/p,e=e*h;e=lift(Mod(e,el));Tr=Tr+z^e);Q=Q*(T-Tr));
Q=component(lift(Q),1);R=0; for(i=0,p,C=component(Q,i+1);C=lift(Mod(C,p));
R=R+x^i*C);F=znorder(Mod(p,el));f=1;v=valuation(F,p);w=valuation(el-1,p);
if(w==v,f=p);print("el=",el," f=",f," R=",R))}
el=29 f=7 R=x^7 + x^6 + 2*x^5 + 5*x + 1
el=43 f=1 R=x^7 + x^6 + 3*x^5 + 3*x^3 + 6*x^2
el=71 f=7 R=x^7 + x^6 + 5*x^5 + 3*x^4 + 2*x^3 + 6*x^2 + 4
el=4943 f=7 R=x^7 + x^ 6 + 3*x^5 + x^4 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 $R_{\ell}$ for large $p$, but any experiment suggests a random distribution of the (non-independent) coefficients (except that of $x^{p-1}$ since $\operatorname{Tr}_{\mathbb{Q}\left(\xi_{\ell}\right) / \mathbb{Q}}\left(\xi_{\ell}\right)=-1$. For $p=3$ the six possible polynomials are of the form $R_{\ell}$. For $p=5$ (resp. $p=7$ ) there are 150 (resp. 17192) possible polynomials.
(i) For $p=5$, we obtain the following end of the calculations (two days of computer; it seems that only 35 distinct polynomials $R_{\ell}$ are available):

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

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

Remark 5.4. It is clear that a large number of polynomials $R_{\ell}$ strengthens Vandiver's conjecture since the corresponding $\mathbf{J}(\ell)=\psi^{-c}(c) \mathrm{g}_{c}(\ell)$ cover sufficiently possibilities modulo $p$, especially since we know that the $\mathbb{F}_{p}$-rank associated to the family of $(\mathbf{J}(\ell))_{\ell \in \mathscr{L}_{p}}$ is probably always $p-4$, but these informations are not "equivalent". Moreover, an assumption about the order of magnitude of $\mathscr{N}_{p}:=\#\left\{R_{\ell}, \ell \in \mathscr{L}_{p}\right\}$ is not necessary to obtain Vandiver's conjecture for $p$; indeed, a single suitable $\ell$ may ensure a positive test for Vandiver's conjecture as shown by the table given in $\S$ 4.2.2.

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

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

## 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 $\mathscr{E}_{\ell}(p)=\emptyset$, may occur conjecturally for all $p$. Possibly, our computations in $\S(4.2 .2)$ show the existence of general properties of the sets $\mathscr{E}_{\ell}(p)$ coming from the fact that all $\ell \in \mathscr{L}_{p}$ intervene (and that these primes are probably independent), which is a new argument compared with classical ones. This is strengthened by the computation of the conjugates of the traces $\operatorname{Tr}_{\mathbb{Q}\left(\xi_{\ell}\right) / F_{\ell}}\left(\xi_{\ell}\right)$, as $\ell \in \mathscr{L}_{p}$ varies (coefficients of the Gauss sums), the fields $\mathbb{Q}\left(\mu_{\ell}\right)$ being, a priori, independent of the arithmetic of $K$.
Remark 6.1. There are two constraints, for the Gauss and Jacobi sums that we have considered, but they only concern the auxiliary prime numbers $\ell \in \mathscr{L}_{p}$ :
(i) The $p$-classes of ideals $\mathfrak{L} \mid \ell, \ell \in \mathscr{L}_{p}$, are all represented with standard densities.
(ii) The ideal factorization of $\tau(\psi)^{p}$ is related to congruences modulo the conjugates of a prime ideal $\mathfrak{L} \mid \ell$ and is canonical (this yields Stickelberger's theorem and its consequences [52, §15.1], [6,55], and [43] for the annihilation of $\mathcal{C} \chi_{\chi_{0}^{*}}^{(p)}$ with generalizations of the Stickelberger ideal). A similar context is that of the $\ell$-adic $\Gamma$-function of Morita.
However, since we consider characters $\psi$ of order $p$, the $p$-adic congruential properties of Gauss sums (or Jacobi sums) do not follow any known law (in our opinion, the classical literature being mute about this).
These fundamental $p$-adic properties of Gauss sums may have crucial consequences in various domains since Vandiver's conjecture is often required; for instance:
In [8] about the Galois cohomology of Fermat curves, in [47] for the root numbers of the Jacobian varieties of Fermat curves, then in several papers on Galois $p$-ramification theory as in $[36,44,45,46]$, or $[53,54]$ in relation with modular forms, then in numerous papers
and books on the theory of deformations of Galois representations as in [2, 37], Iwasawa's theory context and cyclotomy, as in [7] on Ihara series, [5] for $\mu$-invariants in Hida families, [32] for the main conjecture of the Iwasawa theory).
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 $p$ th cyclotomic field (not to mention all the geometrical aspects as the theory of elliptic curves where some analogies can be found, and all the generalizations of the present abelian case over a number field $k \neq \mathbb{Q})$ :

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

Which gives again an example of a basic p-adic problem, analogous to those we have analysed about deep conjectures: Greenberg's conjectures (on Iwasawa theory over totally real fields [22] and on representation theory [24]), p-rationalities of a number field as $p \rightarrow \infty$, generalizations of the conjecture of Ankeny-Artin-Chowla from the conjectural existence of a $p$-adic Brauer-Siegel theorem [20]...
As shown by the evidences given in $\S 5.2$, Vandiver's conjecture may be justified, for $p \gg 0$, by the Borel-Cantelli heuristic, on exceptional features of Gauss sums; but this point of view allows cases of failure of the conjecture, which is not satisfactory for the theoretical foundations of the above quoted fundamental subjects.
To be optimistic (but not very rigorous), one can say that Vandiver's conjecture is true because it holds for sufficiently many prime numbers $[4,9]$ since probabilities may be in $\frac{O(1)}{p^{\lambda(p)}}$, $\lambda(p) \rightarrow \infty$. In a more serious claim, we can say that Vandiver's conjecture holds for almost all prime numbers; the accurate cardinality of the finite set of counterexamples ( $\emptyset$ or not) is (in our opinion) not of algebraic nature nor enlightened by class field theory, Galois cohomology or Iwasawa's theory, but is perhaps accessible by the way of analytical/geometrical techniques or depends on a more general hypothetic "complexity theory" in number theory.

## References

[1] Anglès B and Nuccio F A E, On Jacobi Sums in $\mathbb{Q}\left(\zeta_{p}\right)$, Acta Arithmetica 142(3) (2010) 199-218 https://perso.univ-st-etienne.fr/nf51454h/PDF/jacobi.pdf
[2] Berger T, Oddness of residually reducible Galois representations, Int. J. Number Theory 14(5) (2018) 1329-1345 https://doi.org/10.1142/S1793042118500835
[3] Bayer-Fluckiger E, Emery V and Houriet J, Hermitian Lattices and Bounds in KTheory of Algebraic Integers, Documenta Math Extra Volume Merkurjev (2015) 71-83 https://www.math.uni-bielefeld.de/documenta/vol-merkurjev/
[4] Buhler J P and Harvey D, Irregular primes to 163 million, Math. Comp. 80(276) (2011) 2435-2444 https://doi.org/10.1090/S0025-5718-2011-02461-0
[5] Bellaïche J and Pollack R, Congruences with Eisenstein series and mu-invariants (2018) https://arxiv.org/pdf/1806.04240
[6] Conrad K, Jacobi sums and Stickelberger's congruence, Enseign. Math. 41 (1995) 141-153 http://www.math.uconn.edu/~kconrad/articles/jacobistick.pdf
[7] Coleman R F, Anderson-Ihara theory: Gauss sums and circular units., Algebraic number theory, Adv. Stud. Pure Math. 17 (1989) Academic Press, Boston, MA, 55-72 https://doi.org/10.2969/aspm/01710055
[8] Davis R and Pries R, Cohomology groups of Fermat curves via ray class fields of cyclotomic fields (2018) https://arxiv.org/pdf/1806.08352.
[9] Hart W, Harvey D and Ong W, Irregular primes to two billion, Math. Comp. 86(308) (2017) 3031-3049 https://doi.org/10.1090/mcom/3211
[10] Ellenberg J S and Venkatesh A, Reflection principles and bounds for class group torsion, Int. Math. Res. Not. 2007(1) (2007)
https://doi.org/10.1093/imrn/rnm002
[11] Ghate E, Vandiver's Conjecture via K-theory, Summer School on Cyclotomic fields, Pune (1999) http://www.math.tifr.res.in/\~eghate/vandiver.pdf
[12] Gras G and Jaulent J-F, Sur les corps de nombres réguliers, Math. Z. 202(2) (1989) 343-365 https://eudml.org/doc/174095
[13] Gras G, Étude d'invariants relatifs aux groupes des classes des corps abéliens, Journées Arithmétiques de Caen (Univ. Caen, Caen, 1976) pp. 35-53. Astérisque No. 41-42, Soc. Math. France, Paris (1977) http://www.numdam.org/book-part/AST_1977__41-42__35_0/
[14] Gras G, 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
[15] Gras G, 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
[16] Gras G, Approche p-adique de la conjecture de Greenberg pour les corps totalement réels, Ann. Math. Blaise Pascal 24(2) (2017) 235-291
http://ambp.cedram.org/item?id=AMBP_2017__24_2_235_0
[17] Gras G, On p-rationality of number fields. Applications - PARI/GP programs, Publ. Math. Fac. Sci. Besançon (Algèbre et Théorie des Nombres) (2017/2018) (to appear) https://arxiv.org/pdf/1709.06388
[18] Gras G, Annihilation of $\operatorname{tor}_{Z_{p}}\left(\mathcal{G}_{K, S}^{\mathrm{ab}}\right)$ for real abelian extensions $K / \mathbb{Q}$, Communications in Advanced Mathematical Sciences 1(1) (2018) 5-34
http://dergipark.gov.tr/download/article-file/543993
[19] Gras G, The $p$-adic Kummer-Leopoldt Constant: Normalized p-adic Regulator, Int. J. Number Theory 14(2) (2018) 329-337
https://doi.org/10.1142/S1793042118500203
[20] Gras G, Heuristics and conjectures in direction of a p-adic Brauer-Siegel theorem, Math. Comp. 88(318) (2018-2019) 1929-1965 https://doi.org/10.1090/mcom/3395
[21] Gras G, Practice of the incomplete p-ramification over a number field - History of abelian p-ramification (2019) https://arxiv.org/pdf/1904.10707
[22] Greenberg R, On the Iwasawa invariants of totally real number fields, Amer. J. Math. 98(1) (1976) 263-284 http://www.jstor.org/stable/2373625?
[23] Greenberg R, On the jacobian variety of some algebraic curves, Compositio Math. 42(3) (1980) 345-359 http://www.numdam.org/article/CM_1980__42_3_345_0.pdf
[24] Greenberg R, Galois representations with open image, Annales de Mathématiques du Québec 40(1) (2016) 83-119
https://doi.org/10.1007/s40316-015-0050-6
[25] Gupta S and Don Zagier, On the coefficients of the minimal polynomials of Gaussian periods, Math. Comp. 60(201) (1993) 385-398 https://www.jstor.org/stable/2153175
[26] Ichimura H, Local Units Modulo Gauss Sums, Journal of Number Theory 68(1) (1998) 36-56 https://doi.org/10.1006/jnth. 1997.2206
[27] Ichimura H and Kaneko M, On the Universal Power Series for Jacobi Sums and the Vandiver Conjecture, Journal of Number Theory 31(3) (1989) 312-334
https://core.ac.uk/download/pdf/81986387.pdf
[28] Iwasawa K, A note on Jacobi sums, Symposia Mathematica 15, Academic Press (1975) 447-459.
[29] Jaulent J-F, Unités et classes dans les extensions métabéliennes de degré $n \ell^{s}$ sur un corps de nombres algébriques, Ann. Inst. Fourier (Grenoble) 31(1) (1981) 39-62. http://www.numdam.org/article/AIF_1981__31_1_39_0.pdf/
[30] Kurihara M, Some remarks on conjectures about cyclotomic fields and $K$-groups of $\mathbb{Z}$, Compositio Math. 81(2) (1992) 223-236 http://www.numdam.org/item/CM_1992__81_2_223_0
[31] Kersten I and Michaliček J, On Vandiver's conjecture and $\mathbb{Z}_{p}$-extensions of $\mathbb{Q}\left(\zeta_{p^{n}}\right)$, Journal of Number Theory 32(3) (1989) 371-386
https://doi.org/10.1016/0022-314X (89) 90091-7
[32] Kakde M and Wojtkowiak Z, A note on the main conjecture over $\mathbb{Q}$ (2018) https://arxiv.org/pdf/1812.04360
[33] Lecouturier E, On the Galois structure of the class group of certain Kummer extensions, J. London Math. Soc. 98(2) (2018) 35-58 https://doi.org/10.1112/jlms. 12123
[34] Maire C, Genus theory and governing fields, New York J. Math. 24 (2018) 1056-1067 https://www.emis.de/journals/NYJM/NYJM/nyjm/j/2018/24-50v.pdf
[35] McCallum W G, Greenberg's conjecture and units in multiple $\mathbb{Z}_{p}$-extensions, American Journal of Mathematics 123(5) (2001) 909-930 https://www.jstor.org/stable/25099088
[36] McCallum W G and Sharifi R T, A Cup Product in the Galois Cohomology of Number Fields, Duke Math. J. 120(2) (2003) 269-310 http://math.ucla.edu/~sharifi/pairing.pdf
[37] Mézard A, Obstructions aux déformations de représentations galoisiennes réductibles et groupes de classes, Journal de théorie des nombres de Bordeau 17(2) (2005) 607-618 https://doi.org/10.5802/jtnb. 510
[38] Mihǎilescu P, Turning Washington's Heuristics in Favor of Vandiver's Conjecture, In: Essays in Mathematics and its Applications in Honor of Stephen Smale's 80th Birthday, P. Pardalos, T. Rassias (Eds.), Springer-Verlag (2012) pp. 287-294
http://poivs.tsput.ru/en/Biblio/Publication/11335
[39] The PARI Group, PARI/GP, version 2.9.0, Université de Bordeaux (2016)
[40] Ribet K A, A modular construction of unramified p-extensions of $\mathbb{Q}\left(\mu_{p}\right)$, Invent. Math. 34(3) (1976) 151-162
https://math.berkeley.edu/~ribet/Articles/invent_34.pdf
[41] Ribet K A, Bernoulli numbers and ideal classes, In: L’héritage scientifique de Jacques Herbrand Gaz. Math. 118 (2008) 42-49 https://smf.emath.fr/publications/la-gazette-des-mathematiciens-118-octobre-2008
[42] Schoof R, Class numbers of real cyclotomic fields of prime conductor, Math. Comp. 72(242) (2003) 913-937 https://doi.org/10.1090/S0025-5718-02-01432-1
[43] Schmidt C G, On ray class annihilators of cyclotomie fields, Invent. math. 66(2) (1982) 215-230 https://eudml.org/doc/142878
[44] Sharifi R T, On Galois groups of unramified pro-p extensions, Mathematische Annalen $\mathbf{3 4 2}$ (2) (2008) 297-308 https://doi.org/10.1007/s00208-008-0236-1
[45] Sharifi R T, A reciprocity map and the two-variable p-adic $L$-function, Ann. of Math. (2) 173(1) (2011) 251-300 https://www.jstor.org/stable/29783202
[46] Sharifi R T, Relationships between conjectures on the structure of pro-p Galois groups unramified outside $p$, in: Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), Proc. Sympos. Pure Math. 70 (2002), Amer. Math. Soc., Providence, RI, 275-284
[47] Shu J, Root numbers and Selmer groups for the Jacobian varieties of Fermat curves (2018) https://arxiv.org/pdf/1809.09285
[48] Soulé C, Perfect forms and the Vandiver conjecture, J. Reine Angew. Math. 517 (1999) 209-221 https://doi.org/10.1515/crll.1999.095
[49] Soulé C, A bound for the torsion in the K-theory of algebraic integers, Documenta Math. Extra, vol. Kato (2003) 761-788 http://preprints.ihes.fr/MO2/MO2-82.pdf
[50] Thaine F, On the $p$-part of the ideal class group of $\mathbb{Q}\left(\zeta_{p}+\zeta_{p}^{-1}\right)$ and Vandiver's conjecture, Michigan Math. J. 42(2) (1995) 311-344 https://projecteuclid.org/euclid.mmj/1029005231
[51] Thaine F, On the coefficients of Jacobi sums in prime cyclotomic fields, Transactions of the Amer. Math. Soc. 351(12) (1999) 4769-4790 https://doi.org/10.1090/S0002-9947-99-02223-0
[52] Washington L C, Introduction to cyclotomic fields, Graduate Texts in Mathematics, 83, Springer-Verlag, New York, 1997. xiv+487 pp
[53] Wake P and Erickson C W, Ordinary pseudorepresentations and modular forms, Proc. Amer. Math. Soc. Ser. B 4 (2017) 53-71
https://doi.org/10.1090/bproc/29
[54] Wake P and Erickson C W, Pseudo-modularity and Iwasawa theory, Amer. J. Math. 140(4) (2018) 977-1040 https://arxiv.org/pdf/1505.05128
[55] Weil A, Jacobi sums as "Grössencharaktere", Trans. Amer. Math. Soc. 73 (1952) 487-495 https://www.jstor.org/stable/1990804

Villa la Gardette, 4 Chemin Château Gagnière, F-38520, Le Bourg d’Oisans.
g.mn.gras@wanadoo.fr


[^0]:    Date: June 25, 2019.
    2010 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]:    ${ }^{1}$ The distinction between $\mathfrak{A}^{e_{\theta}} \in I \otimes \mathbb{Z}_{p}$ and $\mathfrak{A}^{e_{\theta}^{\prime}} \in I\left(e_{\theta}^{\prime} \equiv e_{\theta}\left(\bmod p^{N} \mathbb{Z}_{p}[G]\right), N\right.$ large enough) has some importance in practice and programming, provided of a definition of $\mathfrak{A}^{e_{\theta}^{\prime}}$ up to a principal ideal of the form $\left(x^{p}\right)$, for deciding, for instance in the writing $\mathfrak{A}^{e_{\theta}}=:\left(\alpha_{\theta}\right)$, of the " $p$-primarity" of $\alpha_{\theta} \in K^{\times} \otimes \mathbb{Z}_{p}$; whence $\mathfrak{A}^{e_{\theta}^{\prime}}=:\left(\alpha^{\prime}\right)$ where $\alpha_{\theta} \cdot \alpha^{\prime-1} \in\left(K^{\times} \otimes \mathbb{Z}_{p}\right)^{p} \cdot E \otimes \mathbb{Z}_{p}$. This will be used for $\theta \in \mathscr{X}_{+}^{*}$ where $\theta$-components of units do not intervenne, giving $\left(\alpha_{\theta}\right)=(x)^{p} \Leftrightarrow \alpha_{\theta} \in K^{\times p}$.

[^2]:    ${ }^{2}$ If, for instance, $\mathcal{C}_{\chi_{0}} \simeq \mathcal{C}_{\chi_{0}^{*}} \simeq \mathbb{Z} / p \mathbb{Z}$, these prime ideals $\mathfrak{L}$ have density $\left(1-\frac{1}{p}\right)^{2}$; otherwise, if $\mathcal{C}_{\chi_{0}}=1$

