Vandiver’s Conjecture via K-theory

Alexander Stolin

1 Department of Mathematical Sciences, Chalmers University of Technology and the University of Gothenburg, 412 96 Gothenburg, Sweden.

Abstract

From Wikipedia: "In mathematics, the Kummer–Vandiver conjecture, or Vandiver conjecture, states that a prime p does not divide the class number h(R) of the maximal real subfield R of the p-th cyclotomic field. The conjecture was first made by Ernst Kummer in 1849 December 28 and 1853 April 24 in letters to Leopold Kronecker, reprinted in (Kummer 1975, pages 84, 93, 123–124), and independently proposed around 1920 by Philipp Furtwängler and Harry Vandiver. As of 2011, there is no particularly strong evidence either for or against the conjecture and it is unclear whether it is true or false, though it is likely that counterexamples are very rare."

Kummer verified the conjecture for p less than 200, and Vandiver extended this to p less than 600. Harvey (2008) extended this to primes less than $163 \times 10^6$.

In this paper I would like to prove Vandiver’s conjecture and indicate some consequences including the first case of Fermat’s Great Theorem, some properties of the Iwasawa numbers and to present an exact formula for the p-Sylow subgroup of the class group of $Q(\zeta_n)$, where $\zeta_n^{p^{n+1}} = 1$ as an abelian group (OBS! assuming that Vandiver’s conjecture is true, a formula for the class group above as a $\Gamma$-module is well-known. However, the structure of that group as an abelian group remained unknown).

1 Introduction, necessary facts from K-theory

In what follows we will need a number of facts about Picard groups proved in [5].

We will use the following notations. $C_2$ will be the cyclic group of order $p^2$, where $p$ is an odd prime number. $\zeta = \zeta_1$ will be a $p$-th root of unity, while $\zeta_2$ will be a primitive $p^2$-root of unity.
1.1 Review of necessary results of [5]

Let us consider the Picard group of the integer group ring $\mathbb{Z}C_2$. The first observation is that $\text{Pic}(\mathbb{Z}C_2) \cong \text{Pic}(A)$, where $A$ can be presented as a Cartesian product of $\mathbb{Z}[\zeta_1]$ and $\mathbb{Z}[\zeta_2]$ over the local ring $\mathbb{Z}[\zeta_1]/(p) := F$.

The corresponding Mayer–Vietoris sequence reads as

$$0 \to V \to \text{Pic}(A) \to \text{Pic}(\mathbb{Z}[\zeta_2]) \oplus \text{Pic}(\mathbb{Z}[\zeta_1]) \to 0.$$ 

Here $\text{Pic}$, the Picard group, is the same as the projective class group or simply the class group for Dedekind rings. We will use the standard notation $\text{Cl}(D)$.

The group $V$ was computed in [2] for the primes satisfying Vandiver’s conjecture. However, similar computations can be done for any prime. Let us do them. Let $E_i$, $i = 1, 2$ be the group of units of $\mathbb{Z}[\zeta_i]$. Abusing notations let us denote their images in $U(\mathbb{Z}[\zeta_i]/(p))$ also by $E_i$, $i = 1, 2$. Then by definition $V = U(\mathbb{Z}[\zeta_i]/(p))/(E_1 \times E_2)$. Here $U(R)$ is the group of units of an abelian ring $R$.

The following result was proved in [5]:

**Theorem 1.1.** $V = U(\mathbb{Z}[\zeta_1]/(p))/E_1$.

The proof is based on the following useful result:

**Theorem 1.2.** Let $j_i$, $i = 1, 2$ be canonical maps $j : \mathbb{Z}[\zeta_i] \to \mathbb{Z}[\zeta_1]/(p)$ and let $N : \mathbb{Z}[\zeta_2] \to \mathbb{Z}[\zeta_1]$ be the norm map. Then $j_2(a) = j_1(N(a))$.

The structure of $U(\mathbb{Z}[\zeta_1]/(p))$ is well-known:

$$U(\mathbb{Z}[\zeta_1]/(p)) \cong \mathbb{F}_p^* \oplus \mathbb{F}_p^{-2}.$$ 

Here, $\mathbb{F}_p$ is the prime field of characteristic $p$ and $\mathbb{F}_p^*$ is the group of its invertible elements. Now, let us introduce an important number $r_0$. Let $S_i$, $i = 1, 2$ be the Sylow $p$-part of the class group of $\mathbb{Z}[\zeta_i]$. Let us denote the subgroup of the group $\text{Char}(S_1/S_1^p)$ generated by all $\epsilon \in U(\mathbb{Z}[\zeta_1]) : \epsilon \equiv 1 \pmod{p}$ by $(\text{Char}(S_1/S_1^p))_{\epsilon}$.

**Definition 1.3.** $r_0 = \log_p(\#(\text{Char}(S_1/S_1^p))_{\epsilon}) = \log_p(\#\{\epsilon \equiv 1 \pmod{p} \}/\{\epsilon \equiv 1 \pmod{(\zeta_1 - 1)^2}\}.)$.

Now we can formulate an important result:

**Theorem 1.4.** $V \cong \mathbb{F}_p^{p-3+r_0}$.

Another important observation was made in [5]: there exists a splitting map $\text{Cl}(\mathbb{Z}[\zeta_2]) \to \text{Pic}(A)$. Therefore, $\text{Pic}(A) = \text{Pic}(\mathbb{Z}[\zeta_2]) \oplus B$ for a certain group $B$, which will be described explicitly in the next subsection. The Mayer–Vietoris exact sequence reads now as

$$0 \to V \to B \to \text{Pic}(\mathbb{Z}[\zeta_1]) \to 0.$$ 

We continue to review necessary results of [3].
1.2 Invertible modules over $A$

By Milnor’s theory of projective modules over Cartesian products (see [4]), any invertible module over the ring $A$ can be presented as $M(\alpha_1, \alpha_2, h)$, where $\alpha_k \in \mathbb{Z}[\zeta_k]$, $k = 1, 2$ and $h \in U(F)$. The facts below were proved in [5]:

1. $M(\alpha_1, \alpha_2, h) \sim M(q_1\alpha_1, q_2\alpha_2, j_1(q_1^{-1})hj_2(q_2)$, where $q_k \in \mathbb{Z}[\zeta_k]$ are such that $(q_k, p) = 1$;

2. $M(\alpha_1, \alpha_2, h)$ is free if and only if $\alpha_k = (r_k)$, $r_k \in \mathbb{Z}[\zeta_k]$ and $j_1(r_1^{-1})hj_2(r_2) = j_1(\epsilon)$, $\epsilon \in U(\mathbb{Z}[\zeta_1])$;

3. $M(\alpha_1, \alpha_2, h) \otimes M(\beta_1, \beta_2, g) \cong M(\alpha_1\beta_1, \alpha_2\beta_2, hg)$;

4. the map $\psi : Cl(\mathbb{Z}[\zeta_2]) \rightarrow Pic(A)$ defined as $\phi(\alpha) = M(N(\alpha), \alpha, 1)$ ($N$ is the norm map extended to ideals of $\mathbb{Z}[\zeta_2]$) splits the canonical projection $Pic(A) \rightarrow Cl(\mathbb{Z}[\zeta_2])$;

5. $Pic(A) \cong Cl(\mathbb{Z}[\zeta_2]) \oplus B$ for some group $B$ and $V \subset B$.

6. $B$ is generated by invertible modules of the form $M(\alpha, \mathbb{Z}[\zeta_2], h)$.

Note that the Sylow $p$-component of $Pic(\mathbb{Z}[\zeta_1]) = Cl(\mathbb{Z}[\zeta_1])$ is exactly $S_1$. We will denote the Sylow $p$-part of $B$ by $B_p$. Then, the essential part of the exact Mayer–Vietoris reads as follows:

$$0 \rightarrow V \rightarrow B_p \rightarrow S_1 \rightarrow 0.$$

1.3 Numbers $R$, $r$, and fine structure of $B_p$

Let us denote the number of $\mathbb{Z}_p$-generators of the group $S_1$ by $R$. Let us denote by $L \subset S_1$ the subgroup generated by the ideal classes $\alpha \in S_1$ such that $M(\alpha, \mathbb{Z}[\zeta_2], h)$ has exponent $p$ in $Pic(A)$. Of course, $L$ is a subgroup of $S_1$ and $\alpha$ has exponent 1 (this means that $\alpha^p = 1$) in $S_1$.

**Lemma 1.5.** $L$ consists of elements $\alpha \in S_1$ such that $\alpha^p = (q)$ and $q \equiv \epsilon \in U(\mathbb{Z}[\zeta_1]) mod(p)$.

**Remark 1.6.** Changing $q$, we can set $\epsilon = 1$.

**Proof.** A proof easily follows from the properties of $M(\alpha_1, \alpha_2, h)$ above. $\square$

The following result was proved in [5]:

**Lemma 1.7.** $L \cong \text{Char}(S_1/S_1^p) / \text{Char}(S_1/S_1^p, \epsilon)$.

Let us denote the number of of $\mathbb{Z}_p$-generators of $L$ by $r$.

**Corollary 1.8.** $R - r = r_0$. 

3
Corollary 1.9. $B_p \cong \mathbb{F}^{(p-3)/2} \oplus B_1$, where $B_1$ can be described in the following way: it is a $p$-group, its number $\mathbb{Z}_p$-generators is $R$. They are in a one-to-one correspondence with generators $\alpha_i$, $1 \leq i \leq R$ of $S_1$. We denote them by $\beta_1, \ldots, \beta_R$. For $1 \leq i \leq r$ we have $\exp(\beta_i) = \exp(\alpha_i)$ and for $r + 1 \leq i \leq R$ $\exp(\beta_i) = 1 + \exp(\alpha_i)$, where $\exp(x) = n$ means that $x^n = 1$ but $x^{n-1} \neq 1$.

The choice of $\mathbb{Z}_p$-generators of the group $B_1$ is not canonical. However, generators of $\mathbb{F}^{(p-3)/2}$ can be chosen in a canonical way.

Theorem 1.10. Let $S_p$ be a subgroup of $S_1$ consisting of elements of exponent $1$. Then the map $S_p \to V$ determined by $\alpha \to q$, where $\alpha^p = (q)$ is well-defined and its kernel is $L$.

Proof. If we substitute $\alpha$ by $r\alpha$, $r \in \mathbb{Q}(\zeta_1)$, then $q \to r^q q$. Another possible choice of $q$ is $q_0$. These changes will not affect the image of $\alpha$ in $V$. The statement about the kernel follows from the properties of $M(\alpha_1, \alpha_2, h)$ above.

Corollary 1.11. The image of $S_p$ in $V$ is isomorphic to $\mathbb{F}_p^{q_0}$.

We remind the reader that $V \cong \mathbb{F}_p^{\frac{p-2}{2} + q_0}$ and the group $\text{Gal}(\mathbb{Q}(\zeta_1)/\mathbb{Q}) := G$ acts on $V$. The image of $S_p$ is $G$-invariant and therefore, the summand $\mathbb{F}_p^{\frac{p-2}{2}} \subset V \subset B_p$ can be chosen canonically as a $G$-invariant complement to the image of $S_p$ in $V$.

Remark 1.12. The complex conjugation $\sigma \in G$ acts on $V$. Consequently, $V = V_+ \oplus V_-$ with obvious $\pm$-parts $V_\pm$. It easily follows from Kummer’s Lemma ($\epsilon = \zeta_1^k \epsilon_{real}$) that $V_- \cong \mathbb{F}_p^{\frac{p-2}{2}}$ while $V_+ \cong \mathbb{F}_p^{q_0}$. However, it is not difficult to see that $V_+ \neq \text{Im}(S_p)$.

1.4 Action of complex conjugation and further relations between $R$- and $r$-numbers

Let $r_\pm$ be the number of $\mathbb{Z}_p$-generators of $L_\pm$ and let $R_\pm$ be the number of $\mathbb{Z}_p$-generators of $S_1$. Here, $L = L_+ \oplus L_-$ and $S_1 = (S_1)_+ \oplus (S_1)_-$ are defined by action of the complex conjugation $\sigma$.

Lemma 1.13. $\text{Char}(S_1/S_1^p)_+ \subset (\text{Char}(S_1/S_1^p))_+ = \text{Char}((S_1/S_1^p)_-)$. 

Proof. The units defining $\text{Char}(S_1/S_1^p)_+$ are real. It is a consequence of Kummer’s Lemma mentioned above.

Corollary 1.14. $r_- = R_+$, $R_- = r_+ + r_0$.

Proof. Using Lemma 1.13 and the lemma above, we see that $L_- = (\text{Char}(S_1/S_1^p))_- = \text{Char}((S_1/S_1^p)_+)$ what implies the first equality. The second can be proved analogously, alternatively it follows from equalities $R = r + r_0$, $R = R_+ + R_-$, $r = r_+ + r_-$. 

4
Corollary 1.15. First inequality.
\[ R_+ - r_+ \leq r_0 \]

Proof. \[ r_0 = R - r = (R_+ - r_+) + (R_+ - r_-) \geq R_+ - r_- \]

Now, we can reformulate 1.9

Corollary 1.16. • We have two exact sequences
\[ 0 \to V_- = \mathbb{F}_p^{(p-3)/2} \to (B_p)_- \to (S_1)_- \to 0 \]
\[ 0 \to V_+ = \mathbb{F}_p^{r_0} \to (B_p)_+ \to (S_1)_+ \to 0. \]
• \((B_p)_- = \mathbb{F}_p^{\frac{r-p-3}{2} + r} - R \oplus (B_1)_-\)
• The group \((B_1)_-\) can be described as follows: it has \(R_-\) \(\mathbb{Z}_p\)-generators, which are in a one-to-one correspondence with generators \(\alpha_1, \ldots, \alpha_{R_-}\) of \((S_1)_-\). Furthermore, \(r_-\) generators of \((B_1)_-\) have the same exponent as the corresponding generator of \((S_1)_-\) and \(R_- - r_-\) generators have exponent \(\exp(\alpha_i) + 1\).
• \((B_p)_+\) has a similar description but we will not need it.

2 \(B_p\) as a Galois group and the second inequality

Following ideas of [2], let us define the ray ideal group \(H\) as the group of those principal ideals of \(\mathbb{Q}(\zeta_1)\), which possess a generator \(g\) such that \(g \equiv 1 \mod(p)\).

Let us denote \(\mathbb{Q}(\zeta_n), \zeta_n^p = 1\) by \(\mathbb{K}_{n-1}\). Sometimes we denote \(\mathbb{K}_0\) simply by \(\mathbb{K}\). Let \(\mathcal{M}/\mathbb{K}\) be the Sylow \(p\)-part of the ray class field extension associated with the group \(H\). Hence, \(\mathcal{M}/\mathbb{K}\) is an abelian extension with the Galois group \(\text{Gal}(\mathcal{M}/\mathbb{K}) \cong (I_0(\mathbb{K})/H)_p\), where \(I_0(\mathbb{K})\) is the group of ideals of \(\mathbb{K}\) prime to \(p\) and \((I_0(\mathbb{K})/H)_p\) is the Sylow \(p\)-subgroup of the finite group \(I_0(\mathbb{K})/H\) (the group of all ideals of \(\mathbb{K}\) will be denoted by \(I(\mathbb{K})\)).

We remind the reader that groups \(B\) and \(B_p\) were defined in subsection 1.2.

Theorem 2.1. The map \(M(\alpha, \mathbb{Z}[\zeta_2], h) \to h^{-1}\alpha\) defines isomorphisms \(B \cong I_0(\mathbb{K})/H\) and \(B_p \cong (I_0(\mathbb{K})/H)_p\).

Proof. Clearly this map is surjective. Let us prove that the map is injective. Indeed, its kernel consists of elements such that \(h^{-1}\alpha\) is a principal ideal, which possesses a generator \(g \equiv 1 \mod(p)\). However, it follows from the properties of invertible modules over the ring \(A\) (subsection 1.2) that such \(M(\alpha, \mathbb{Z}[\zeta_2], h)\) is free.

Corollary 2.2. Let \(\mathcal{L}\) be the Sylow \(p\)-part of the Hilbert class field of \(\mathbb{K}\).

• Then \(\text{Gal}(\mathcal{L}/\mathbb{K}) \cong S_1\), \(\text{Gal}(\mathcal{M}/\mathcal{L}) \cong V\), and the Mayer-Vietoris exact sequence \(0 \to V \to B_p \to S_1\) becomes the exact sequence of the Galois groups of the tower of field extensions \(\mathbb{K} \subset \mathcal{L} \subset \mathcal{M}\).
• Consequently, there are exactly \( R - r \) cyclic extensions \( M_\alpha/K \) such that\( M_\alpha \subset M \), \( \text{Gal}(M_\alpha/K) \) is a cyclic group of order \( p^k, k \geq 2 \) and \( \text{Gal}(M_\alpha/M_\alpha \cap \mathbb{L}) \) is cyclic of order \( p \) or if you wish \( \text{Gal}((M_\alpha \cap \mathbb{L})/K) \) is cyclic of order \( p^{k-1} \).

• Let \( M_- \) be the extension of \( K \) with the Galois group \( (B_p)_- \). Then there are \( R_- - r_- \) cyclic extensions \( M_\alpha/K \) such that \( M_\alpha \subset (M)_- \), \( \text{Gal}(M_\alpha/K) \) is a cyclic group of order \( p^k, k \geq 2 \) and \( \text{Gal}(M_\alpha/M_\alpha \cap \mathbb{L}) \) is cyclic of order \( p \).

Now, we will need the diagram of field extensions as illustrated below.

\[
\begin{align*}
\mathbb{K}_n & \cdot M \\
\mathbb{K}_n & \cdot L \\
\mathbb{K}_n & \\
\mathbb{K} &= \mathbb{K}_0 \\
M & \\
L & \\
\end{align*}
\]

**Lemma 2.3.** \( \mathbb{K}_n \cap M = \mathbb{K} \)

*Proof.* We follow the proof of Lemma 4.4 of [2]. If \( \mathbb{K}_n \cap M \neq \mathbb{K} \), then \( \mathbb{K}_n \cap M \supset \mathbb{K}_1 \). Therefore, it is sufficient to prove that \( \mathbb{K}_1 \) is *not contained in \( M \). Indeed, \( M \) is associated with the ray group \( H \) defined above. As it is well-known, \( \mathbb{K}_1 \) is a class field over \( \mathbb{K} = \mathbb{K}_0 \) associated with the ray group

\[
P = \{ \alpha \in I(\mathbb{K}) : \text{Norm}(\alpha) \equiv 1 \ mod(p^2) \},
\]

(see [2] and references therein). Here, the norm \( \text{Norm} \) acts from \( \mathbb{K} \) to \( \mathbb{Q} \). Hence, we must prove that \( H \not\subseteq P \).

Let us choose \( \beta = (1 + p) \). Clearly, \( \beta \in H \). On the other hand,

\[
\text{Norm}(1 + p) = (1 + p)^{p-1} \equiv 1 + (p - 1)p \ mod(p^2) \neq 1 \ mod(p^2).
\]

Hence, \( \beta \not\in P \) and \( H \not\subseteq P \). The lemma is proved. \( \square \)

**Corollary 2.4.** \( \text{Gal}(\mathbb{K}_n \cdot M/\mathbb{K}_n) \cong \text{Gal}(M/\mathbb{K}) \).
The main aim of this section is to prove the second inequality namely \( r_0 \leq R_- - r_- \). To do this, we will study \((\text{Gal}(\mathbb{K}_n : \mathbb{M}/\mathbb{K}_n))_- = (\text{Gal}(\mathbb{M}/\mathbb{K}))_- = (B_p)_-\).

We make an important

**Remark 2.5.** Since \( p \) is odd, we have \((B_p)_- \cong ((I_0(\mathbb{K})/H)_p)_- \cong ((I_0(\mathbb{K})/H)_p)_-\), where \( H \) is the group of those principal ideals of \( \mathbb{K}_0 = \mathbb{Q}(\zeta_1) \), which possess a generator \( g \) such that \( g \equiv 1 \mod (\zeta_1 - 1)^p \). Indeed, there is an obvious surjection \((I_0(\mathbb{K})/H)_p \twoheadrightarrow (I_0(\mathbb{K})/H)_p\) and its kernel is the ideal \((p + 1)\), which is contained in \((I_0(\mathbb{K})/H)_p\). Hence, the odd parts are isomorphic.

From now on we will use notation \( H_n \) for the group of those principal ideals of \( \mathbb{K}_n = \mathbb{Q}(\zeta_{n+1}) \), which possess a generator \( g \) such that \( g \equiv 1 \mod (\zeta_{n+1} - 1)^{p^{m+1}} \) \( (H_0 = H) \).

Let \( M_n/\mathbb{K}_n \) be the Sylow \( p \)-part of the ray class field extension associated with the group \( H_n \). Hence, \( M_n/\mathbb{K}_n \) is an abelian extension with the Galois group \( \text{Gal}(M_n/\mathbb{K}_n) \cong (I_0(\mathbb{K}_n)/H_n)_p \), where \( I_0(\mathbb{K}_n) \) is the group of ideals of \( \mathbb{K}_n \) prime to \( p \) and \((I_0(\mathbb{K}_n)/H_n)_p \) is the Sylow \( p \)-subgroup of the finite group \( I_0(\mathbb{K}_n)/H_n \). Denote the group \( \text{Gal}(\mathbb{K}_n/\mathbb{K}_0) \) by \( G_n \). It naturally acts on \( I(\mathbb{K}_n)/H_n \). Let us remind the reader a standard notation: if a cyclic group \( A \) generated by \( a \in A \) acts on a group \( B \), then \( B^A = \{ b \in B : a(b) = b \} \).

Our next goal is to prove

**Theorem 2.6.** \( H^0(G_n, I_0(\mathbb{K}_n)/H_n) = (I_0(\mathbb{K}_n)/H_n)^{G_n} = I_0(\mathbb{K}_0)/H_0 \).

**Proof.** Obviously, it is sufficient to prove that

\[
H^0(G, I_0(\mathbb{K}_m)/H_m) = (I_0(\mathbb{K}_m)/H_m)^{G} = I_0(\mathbb{K}_{m-1})/H_{m-1},
\]

where \( G = \text{Gal}(\mathbb{K}_m/\mathbb{K}_{m-1}) \).

For this will need an idelic interpretation of \( I_0(\mathbb{K}_m) \). Let \( J(k) \) be the idele group of a global field \( k \). For any valuation \( v \), let \( k_v \) be the corresponding completion.

Let \( S \) be a finite subset of the set of all valuations of \( k \).

Denote by \( J^S(k) \subset J(k) \) the subgroup of elements which have 1 at all \( v \)-components, \( v \in S \) and let \( U^S(k) \subset J^S(k) \) be a subgroup, which has a unit of \( \omega_v \) at any \( v \)-component (clearly \( v \notin S \)).

In our case, for all \( \mathbb{K}_n, S \) will contain two elements: the archimedean valuation and \( \omega_n = (\zeta_n + 1 - 1) \). We have a surjection \( J^S(\mathbb{K}_m) \twoheadrightarrow I_0(\mathbb{K}_m) \) with the kernel \( U^S(\mathbb{K}_m) \). Consequently, we have a surjection \( J^S(\mathbb{K}_m) \twoheadrightarrow I_0(\mathbb{K}_m)/H_m \) with the kernel \( (\mathbb{K}_m \cap U_{m,\omega_m}) \times U^S(\mathbb{K}_m) \). Here \( \mathbb{K}_m = \mathbb{K}_m \} \setminus \{ 0 \}, U_{m,\omega_m} \) is the set of units of \( (\mathbb{K}_m)_\omega_m \), which are congruent 1 \( \text{modulo} \ \omega_m^{p^{m+1}} = (\zeta_m + 1 - 1)^{p^{m+1}} \), and \( \mathbb{K}_m \) is embedded into \( J^S(\mathbb{K}_m) \) diagonally.

So, we have an exact sequence of \( G \)-modules:

\[
0 \rightarrow (\mathbb{K}_m \cap U_{m,\omega_m}) \rightarrow J^S(\mathbb{K}_m)/U^S(\mathbb{K}_m) \rightarrow I_0(\mathbb{K}_m)/H_m \rightarrow 0 \quad (1)
\]
Let us prove first that \( H^0(J^S(\mathbb{K}_m)/U^S(\mathbb{K}_m)) = (J^S(\mathbb{K}_m)/U^S(\mathbb{K}_m))^G = J^S(\mathbb{K}_{m-1})/U^S(\mathbb{K}_{m-1}) \). To do this, we consider another exact sequence of \( G \)-modules: \( 0 \to U^S(\mathbb{K}_m) \to J^S(\mathbb{K}_m) \to J^S(\mathbb{K}_m)/U^S(\mathbb{K}_m) \to 0. \)

Clearly, we have

- \((U^S(\mathbb{K}_m))^G = U^S(\mathbb{K}_{m-1})\);
- \((J^S(\mathbb{K}_m))^G = J^S(\mathbb{K}_{m-1})\);
- \(H^1(G, U^S(\mathbb{K}_m)) = \{1\}\) because for all valuations \( v \notin S \) of \( \mathbb{K}_m \), local extensions \((\mathbb{K}_m)_v/(\mathbb{K}_{m-1})_v\) are unramified. Here the valuation \( \tilde{v} \) of \( \mathbb{K}_{m-1} \) lies under \( v \) (see [1] for details).

Now, the corresponding exact sequence of cohomology groups reads as

\[
0 \to U^S(\mathbb{K}_{m-1}) \to J^S(\mathbb{K}_{m-1}) \to (J^S(\mathbb{K}_m)/U^S(\mathbb{K}_m))^G \to 0,
\]

what proves that \((J^S(\mathbb{K}_m)/U^S(\mathbb{K}_m))^G = J^S(\mathbb{K}_{m-1})/U^S(\mathbb{K}_{m-1}).\)

Let us return to the exact sequence (1) and the corresponding exact cohomology sequence:

\[
0 \to (\mathbb{K}_m^* \cap U_{m,\omega})^G \to J^S(\mathbb{K}_{m-1}) \to (J^S(\mathbb{K}_m)/U^S(\mathbb{K}_m))^G \to H^1(G, \mathbb{K}_m^* \cap U_{m,\omega}).
\]

The following observation is clear: \((\mathbb{K}_m^* \cap U_{m,\omega})^G \) consists of the elements of \( x \in \mathbb{K}_{m-1} \) such \( x \equiv 1 \mod \omega_m^{p+1} \). Since \( \omega_m^{p+1} = \omega_{m-1} \), we deduce that \((\mathbb{K}_m^* \cap U_{m,\omega})^G = \mathbb{K}_{m-1}^* \cap U_{m-1,\omega_{m-1}}^G \).

Thus, the statement of the theorem will follow from that of \( H^1(G, \mathbb{K}_m^* \cap U_{m,\omega}) = \{1\}\). Let us prove this.

Any 1-cocycle is generated by some \( x \in \mathbb{K}_m^* \cap U_{m,\omega} \) such that \( \text{Norm}_{\mathbb{K}_m/\mathbb{K}_{m-1}}(x) = 1 \). Hilbert 90 immediately implies that \( x = \sigma(a)/a \) for some \( a \in \mathbb{K}_m^* \) (\( \sigma \) is a generator of \( G \)).

On the other hand, the same \( x \) generates a 1-cocycle of \( Z^1(G, U_{m,\omega}) \). Let us prove that \( H^1(G, U_{m,\omega}) \) is trivial. Indeed, let \( u \in U_{m,\omega} \) Then the series \( \log(u) \) converges that provides an isomorphism \( U_{m,\omega} \cong \omega_{m+1} \cdot O((\mathbb{K}_m)_\omega) \). Here, \( O((\mathbb{K}_m)_\omega) \) denotes the ring of integers of the local field \( k_v \). Since \( O((\mathbb{K}_m)_\omega) \) is a free \( G \)-module, we obtain \( H^1(G, U_{m,\omega}) \) is trivial. Consequently, \( x = \sigma(u)/u \) for some \( u \in U_{m,\omega} \).

Now, it is not difficult to finish the proof of the theorem. We have \( x = \sigma(a)/a = \sigma(u)/u \). Therefore, \( t = a/u \in (\mathbb{K}_{m-1})_\omega \). We can find \( a_1 \in \mathbb{K}_{m-1}^* \) and \( u_1 \in U_{m-1,\omega_{m-1}} \) such that \( t = a_1/u_1 \) because \( \mathbb{K}_{m-1} \) is dense in \((\mathbb{K}_{m-1})_\omega \). Finally we get: \( b = a/a_1 = u/u_1 \in \mathbb{K}_m^* \cap U_{m,\omega} \) and \( \sigma(b)/b = \sigma(a)/a = x \).

Thus, \( H^1(G, U_{m,\omega}) \) is trivial and the theorem is proved. \( \square \)

The main result of the section is

**Theorem 2.7.** \( R_- - r_- \geq r_0 \).

**Proof.** The idea of the proof is to find \( r_0 \) cyclic extensions \( M_\alpha \) of \( \mathbb{K}_n \) such that...
1. $\mathcal{M}_\alpha \subset \mathcal{M} \cdot \mathcal{K}_n$;

2. $\text{Gal}(\mathcal{M}_\alpha/\mathcal{K}_n)$ is an odd group with respect to the natural action of the complex conjugation;

3. The extension $\mathcal{M}_\alpha/\mathcal{K}_n$ ramifies at $\omega_n$.

There are obvious candidates for $\mathcal{M}_\alpha$, namely $\mathcal{M}_\alpha = \mathcal{K}_n(\epsilon^{1/p^{m_i+1}})$, where $\epsilon$’s are units of $\mathbb{K} = \mathbb{K}_0$, which are local $p^{m_i}$-powers ($m_i > 0$) in $\mathbb{K}_{\omega_0}$ but not $p$-powers in $\mathbb{K}$. We have exactly $r_0$ such units. Let $m = m_1$. Let $\gamma = \epsilon^{1/p^m} \in \mathbb{K}_{\omega_0}$.

Then, the extension $\mathbb{K}_{\omega_0}(\gamma^{1/p})/\mathbb{K}_{\omega_0}$ ramifies and consequently the extension $\mathcal{M}_\alpha = \mathcal{K}_n(\gamma^{1/p})/\mathcal{K}_{\omega_0}$ ramifies. Let us explain this.

**Explanation 2.8.** Indeed, this extension cannot become unramified of degree $p$ because it contains a ramified subextension $\mathbb{K}_{\omega_0}(\gamma^{1/p})/\mathbb{K}_{\omega_0}$.

Then, the only possibility is that $\mathcal{M}_\alpha = \mathcal{K}_n(\gamma^{1/p})$. Taking $n$ minimal with this property, we get following relations between degrees:

$$[(\mathcal{K}_n - 1)_{\omega_n - 1}(\gamma^{1/p}) : (\mathcal{K}_n - 1)_{\omega_n - 2}] = [(\mathcal{K}_n : (\mathcal{K}_n - 1)_{\omega_n - 1} = p].$$

Further, $(\mathcal{K}_n - 1)_{\omega_n - 1}(\gamma^{1/p}) \subset (\mathcal{K}_n)_{\omega_n}(\gamma^{1/p})$ and hence, $(\mathcal{K}_n - 1)_{\omega_n - 1}(\gamma^{1/p}) = (\mathcal{K}_n)_{\omega_n} = (\mathcal{K}_n - 1)_{\omega_n - 1}(\gamma^{1/p})$. So, $\zeta_n \gamma^{-1} = r^p$, $r \in (\mathcal{K}_n - 1)_{\omega_n - 1}$. The latter equality cannot be true even modulo $(\zeta_n - 1)^2$ that completes the explanation of the third statement.

The second statement is clear because by Kummer’s Lemma $\epsilon$ is real and consequently, $\text{Gal}(\mathcal{K}_n(\epsilon^{1/p^{m+1}})/\mathcal{K}_n) = (\text{Gal}(\mathcal{K}_n(\epsilon^{1/p^{m+1}})/\mathcal{K}_n))_\epsilon$.

It remains to prove the first statement.

**Claim 1:** $\mathcal{K}_n(\epsilon^{1/p^{m+1}}) \subset \mathcal{M}_\alpha$.

To prove this claim we have to use some facts of the global class field theory (see [1]). Let $F_{\mathcal{K}_n(\epsilon^{1/p^{m+1}})/\mathcal{K}_n} : I_0(\mathcal{K}_n) \rightarrow \text{Gal}(\mathcal{K}_n(\epsilon^{1/p^{m+1}})/\mathcal{K}_n)$ be the map constructed using Frobenius maps. The Artin map (see again [1])

$$\psi_{\mathcal{K}_n(\epsilon^{1/p^{m+1}})/\mathcal{K}_n} : J(\mathcal{K}_n) \rightarrow \text{Gal}(\mathcal{K}_n(\epsilon^{1/p^{m+1}})/\mathcal{K}_n)$$

satisfies

- $\psi_{\mathcal{K}_n(\epsilon^{1/p^{m+1}})/\mathcal{K}_n}(x) = \Pi_v \psi_v(x_v)$, here $x = (x_v) \in J(\mathcal{K}_n)$ and $\psi_v$ are local Artin maps;

- $\psi_{\mathcal{K}_n(\epsilon^{1/p^{m+1}})/\mathcal{K}_n}(x) = F_{\mathcal{K}_n(\epsilon^{1/p^{m+1}})/\mathcal{K}_n}(x^S)$ where $x \in J(\mathcal{K}_n)^{S}$ and $(x)^S$ is the image of $x$ under the canonical map $J(\mathcal{K}_n)^{S} \rightarrow I_0(\mathcal{K}_n)$;

- $\psi_{\mathcal{K}_n(\epsilon^{1/p^{m+1}})/\mathcal{K}_n}(1) = 1$.

We proceed to the proof of Claim 1. Let $(q) \in H_n$. We have to prove that $F_{\mathcal{K}_n(\epsilon^{1/p^{m+1}})/\mathcal{K}_n}((q)) = \epsilon^{1/p^{m+1}}$.

Let us present $q \in \mathcal{K}_n^* \subset J(\mathcal{K}_n)$ as $q = (q)^S q_{\omega_n}$, where $(q)^S = (q, \ldots, q, \ldots) \in J(\mathcal{K}_n)^S$ and $q_{\omega_n} = q \in (\mathcal{K}_n)_{\omega_n}$. We have (denoting the Artin map by simply $\psi$, similarly for $F$):

$$1 = \psi((q)^S) \cdot \psi_{\omega_n}(q) = F((q)) \cdot \psi_{\omega_n}(q), \quad (q) \in H_n \subset I_0(\mathcal{K}_n).$$
Therefore, proving $F((\epsilon)) (\epsilon^{1/p^{m+1}}) = \epsilon^{1/p^{m+1}}$ is equivalent to $\psi_{\omega_n}(q)(\epsilon^{1/p^{m+1}}) = \epsilon^{1/p^{m+1}}$. The latter is equivalent to that of $(\epsilon, q)_{m+1} = 1$. Here, $(\cdot, \cdot)_k$ is the $\omega_n$-local norm residue symbol with values in $p^k$-roots of unity. Taking into account that $\epsilon = \gamma_p^m$ we deduce that $(\epsilon, q)_{m+1} = (\gamma, q)_1$. The latter is 1 because of the following exercise from [1]:

$$(1 - \omega_n^k, 1 - \omega_n^l)_1 = (1 - \omega_n^k, 1 - \omega_n^l)_1 \cdot (1 - \omega_n^l, 1 - \omega_n^{k+l})^{-1} \cdot (1 - \omega_n^{k+l}, \omega_n)_1^{-1}$$

In our case it is sufficient to consider $k > 1$ and $l \geq p^{n+1}$. Then $1 - \omega_n^{k+l}$ is a $p$-power and all three factors in the right hand side are equal to 1. Claim 1 is proved.

**Claim 2:** $\mathbb{K}_n(\epsilon^{1/p^{m+1}}) \subset M \cdot \mathbb{K}_n$.

Let $\sigma_n$ be a generator of $G_n = \text{Gal}(\mathbb{K}_n/\mathbb{K})$. We have proved that $\mathbb{K}_n(\epsilon^{1/p^{m+1}}) \subset M_n$. So, $\text{Gal}(\mathbb{K}_n(\epsilon^{1/p^{m+1}})/\mathbb{K}_n)$ is a factor of $\text{Gal}(M_n/\mathbb{K}_n)$. Since $\sigma_n(\epsilon) = \epsilon$, we deduce that $\text{Gal}(\mathbb{K}_n(\epsilon^{1/p^{m+1}})/\mathbb{K}_n)$ is a factor of $\text{Gal}(M_n/\mathbb{K}_n)$ by Theorem 2.6 (because $\text{Gal}(M_n/\mathbb{K}_n) = I_0(\mathbb{K}_n)/H_n$ and $\text{Gal}(M \cdot \mathbb{K}_n/\mathbb{K}_n) = I_0(\mathbb{K})/H_n$). Therefore, $\mathbb{K}_n(\epsilon^{1/p^{m+1}}) \subset M \cdot \mathbb{K}_n$. The first statement is proved.

Hence, we have constructed $r_0$ extensions of $\mathbb{K}_n$ satisfying conditions 1, 2, 3 above. Corollary 2.2, Lemma 2.3, and Corollary 2.4 imply that the total number of such extensions is $R_- - r_-$ that implies the required inequality. The theorem is proved.

**Corollary 2.9.** $R_- - r_- = r_0$

**Corollary 2.10.** $r_0 = r_+ = R_+$

**Proof.** We have: $R_- - r_- = r_0 = R - r = (R_- - r_-) + (R_+ - r_+)$. Therefore, $R_+ = r_+$. The equality $R_+ = r_+$ was proved in the first section of the paper. \)

## 3 Proof of Vandiver’s conjecture

After the corollary above, in order to prove Vandiver’s conjecture we have to prove that $r_+ = 0$. This will be done using Leopoldt’s conjecture for the field $\mathbb{K}$ (in this case it is known that the conjecture is true). Corollary 1.16 implies

**Lemma 3.1.** $\frac{(B_p)_-}{((B_p)_-)^p} \cong \mathbb{F}_p^{p-3+r_-}$

In what follows, we will use the group $S_p$ defined in Theorem 1.10.

**Lemma 3.2.** Let a real number $d \in \mathbb{K}$ satisfy $(d) = \alpha^p$ for some ideal $\alpha \subset \mathbb{K}$. Then $\mathbb{K}(d^{1/p}) \subset M$.

**Proof.** Exactly as in the proof of Claim 1 from the previous section, we have to prove that $(d, q)_1 = 1$ for any $q \equiv 1 \text{mod}(p)$. Since $d$ is real, it satisfies $d \equiv 1 \text{mod}(\zeta_1 - 2)$ and the already mentioned in the previous section exercise from [1] completes the proof. \)
Corollary 3.3. Let \( (d) = \alpha^p \) for some ideal \( \alpha \subset \mathbb{K} \) and \( d \) be real. Let the class of \( \alpha \) is such that \( [\alpha] \in (S_p)_+ \). Then, such \( d \) induces a character of \( (B_p)_-/(S_p)_- )^p \) (Kummer’s duality).

Proof. Clearly, \( d \) induces a character of \( (B_p)/((B_p))^p \). Since \( d \) is real, this character is a character of \( (B_p)_-/(S_p)_- )^p \).

Theorem 3.4. Let \( (d) = \alpha^p \) for some ideal \( \alpha \subset \mathbb{K} \) such that \( [\alpha] \) is an element of \( (S_p)_+ \). Then \( d \) induces a character of \( (B_p)_-/(S_p)_- )^p \) and \( d \) is a local \( p \)-power in \( \mathbb{K}_\omega_0 \).

Proof. Let \( \mathbb{K}^+ \) be the real subfield of \( \mathbb{K} \). The group \( S_1(\mathbb{K}) \) was defined in the section 1.1 and it was the \( p \)-Sylow component of the class group. Let us similarly define \( S_1(\mathbb{K}^+) \). It was proved in [2] that the inclusion \( \mathbb{K}^+ \to \mathbb{K} \) induces an isomorphism \( S_1(\mathbb{K}^+) \to (S_1(\mathbb{K}))_+ \) (Lemma 4.5 and further references to papers by Iwasawa). Moreover, it follows from the proof of Lemma 4.5 that the ideal \( r\alpha, r \in \mathbb{K}^+ \), can be chosen to be the extension in \( \mathbb{K} \) of some ideal in \( \mathbb{K}^+ \). It follows that \( d = d_1r^p \), where \( d_1 \) is real and \( r \) is a unit. Using the change \( d \to \zeta_1 d \), we can achieve that \( d \equiv 1 \mod (\zeta_1 - 1)^2 \). Then \( r \) becomes a real unit and \( d = d_2r^p \) with real \( d_2 = d_1 r \). Hence, Then \( d \) induces a character of \( (B_p)_-/(S_p)_- )^p \).

Let us prove that \( d \) is locally a \( p \)-power. Indeed, the fact that \( R_+ = r_+ \) (Corollary 2.10) implies that \( d \) can be chosen \( d \equiv 1 \mod (p) \). It was proved in [3], Lemma 2, that then \( d \equiv 1 \mod (\zeta_1 - 1)^p \). To complete the proof of the fact that \( d \) is a local \( p \)-power, we need one step further, namely to prove that \( d \equiv 1 \mod (\zeta_1 - 1)^{p+1} \). We have \( d = d_2r^p \), where \( d_2 \) is real. Changing \( r \to \zeta r \) we can achieve \( r \equiv 1 \mod (\zeta_1 - 1)^2 \) and \( r^p \equiv 1 \mod (\zeta_1 - 1)^{p+1} \). Since \( d \equiv 1 \mod (\zeta_1 - 1)^p \) and \( d_2 \) is real, we see that \( d_2 \equiv 1 \mod (\zeta_1 - 1)^{p+1} \) and consequently \( d \equiv 1 \mod (\zeta_1 - 1)^{p+1} \).

Corollary 3.5. The character group of \( (B_p)_-/(S_p)_- )^p \) is generated by real units of \( \mathbb{K} \) (we have \( \frac{p-3}{2} \) ones) and the set \( \{d_i\} \) defined above (we have \( r_+ = r_- \) ones).

Now, we can prove Vandiver’s conjecture.

Theorem 3.6. \( r_+ = 0 \).

Proof. Let \( U_1 \) be a subgroup of \( U(\mathbb{Z}_p[\zeta_1])^+ \) ("real" \( p \)-adic units) generated by elements congruent \( 1 \mod (\zeta_1 - 1)^2 \). Let \( W \subset U_1 \) be the subgroup of elements of norm 1, i.e., \( \text{Norm}_{\mathbb{K}/\mathbb{Q}}(w) = 1 \). It is well-known that \( W \) is a \( \mathbb{Z}_p \)-module of rank \( \frac{p-3}{2} \). Let \( E \) be a group of real units of \( \mathbb{Z}[\zeta_1] \) and let \( \bar{E} \) be its closure in \( W \). By Leopoldt’s conjecture \( \bar{E} \) is a \( \mathbb{Z}_p \)-module of rank \( \frac{p-3}{2} \). Therefore, \( W/\bar{E} \) is a finite \( \mathbb{Z}_p \)-module (of rank at most \( \frac{p-3}{2} \)).

Let us "improve" \( d_i \) from the corollaries above. We have: \( \text{Norm}_{\mathbb{K}/\mathbb{Q}}(d_i) = q_i^p \) (Explanation: \( (d_i) = \alpha^p_i \); \( \text{Norm}_{\mathbb{K}/\mathbb{Q}}(\alpha_i) = (t_i) = \pm t_i \in \mathbb{Q} \) and so, \( q_i = t_i \) or \( q_i = -t_i \)). Then \( \text{Norm}_{\mathbb{K}/\mathbb{Q}}(d_i^{-1}q_i^{-p}) = q_i^{-p} = 1 \). Consequently, \( h_i = d_i^{-1}q_i^{-p} \in W \) and \( h_i \) generate a character of \( (B_p)_-/(S_p)_- )^p \).
Since $h_i$ is a local $p$-power, we can find $r_i \in K$ with $\text{Norm}_{K/Q}(r_i) = 1$ such that $h_i r_i^p \in \bar{E}$, which is generated by real units of $\mathbb{Z}[\zeta_1]$ as a $\mathbb{Z}_p$-module. Therefore, the group of characters of $(B_p)_-/(B_p)_-^p$ is a factor-module of $\bar{E}$, which is a free $\mathbb{Z}_p$-module of rank $\frac{p^2 - 3}{2}$. However, $(B_p)_-/(B_p)_-^p$ has rank $\frac{p^2 - 3}{2} + r_-$ as a $\mathbb{Z}_p$-module. It follows that $r_+ = r_- = 0$. The theorem and Vandiver’s conjecture are proved.

References

[1] Cassels, J. W. S., Fröhlich, A. Algebraic Number Theory. Academic Press, London and New York, 1967.

[2] Kervaire, M., Murthy, M. P. On the projective class group of cyclic groups of prime power order. Comment. Math. Helvetici, 52(1977).

[3] Mazur, Barry; Wiles, Andrew (1984). "Class fields of abelian extensions of $\mathbb{Q}$", Inventiones Mathematicae, 76 (2).

[4] Milnor, J. Introduction to algebraic $K$-theory. Ann. of Math. Stud., v. 72, Princeton Univ. Press, Princeton, NJ, 1971.

[5] Stolin, A. An explicit formula for the Picard group of the cyclic group of order $p^2$. Proc. Amer. Math. Soc. 121 (1994).

[6] Stolin, A. On the Picard group of the integer group ring of the cyclic $p$-group and certain Galois groups. J. Number Theory 72 (1998).

[7] Stolin, A. Kervaire–Murthy conjecture, Ullom’s inequality and Iwaswa numbers. [arXiv:1003.1871]

[8] Washington, L. Introduction to Cyclotomic Fields. Springer. Graduate Texts in Mathematics 83.