ON THE NON p-RATIONALITY AND IWASAWA INVARIANTS OF CERTAIN REAL QUADRATIC FIELDS

PEIKAI QI AND MATT STOKES

Abstract. Let p be an odd prime, and $m, r \in \mathbb{Z}^+$ with m coprime to p. In this paper we investigate the real quadratic fields $K = \mathbb{Q}(\sqrt{m^2p^{2r}+1})$. We first show that for $m < C$, where constant C depends on p, r, the fundamental unit ε of K satisfies the congruence $\varepsilon^{p-1} \equiv 1 \pmod{p^2}$, which implies that K is a non p-rational field. Varying r then gives an infinite family of non p-rational fields. When $m = 1$ and p is a non-Wieferich prime, we use a criterion of Fukuda and Komatsu [12] to show that if p does not divide the class number of K, then the Iwasawa invariants for a cyclotomic $\mathbb{Z}_p$-extension of K vanish. We conjecture that there are infinitely many r such that p does not divide the class number of K.

1. Introduction

1.1. **p-Rational Fields.** Let F be a number field, and p a prime number. Let S be the set of primes of F above p and let L be the maximal pro-p abelian extension of F unramified outside of S. Then $\mathrm{Gal}(L/F) \cong \mathbb{Z}_p^\rho \times \mathcal{T}_F$, where ρ is a positive integer and $\mathcal{T}_F$ is the torsion subgroup of $\mathrm{Gal}(L/F)$. It is known [46, Theorem 13.4] that $\rho \geq r_2 + 1$, where $2r_2$ is the number of complex embeddings $F \hookrightarrow \mathbb{C}$. Leopoldt's conjecture predicts that $\rho = r_2 + 1$. In this paper, we always assume Leopoldt's conjecture holds for the number field F and prime p. We say F is p-rational if $\mathcal{T}_F$ vanishes. The concept of p-rationality has its origins in ramification theory, where it is closely related to the Galois cohomology of maximal pro-p extensions unramified outside the primes above p [36] [37] [40].

The study of p-rational fields is closely related to Leopoldt's conjecture and to pro-p extensions with restricted ramification, going back to the work of Shafarevich and Wingberg [43, 48]. The notion was later systematically developed by Movahhedi and Nguyen Quang Do [36, 37]. Related developments include Jaulent's work on l-adic independence [25], the study of p-rationality and p-regularity by Jaulent and Nguyen Quang Do [26], and the relative notion of S-rationality introduced by Jaulent and Sauzet [27]. More recently, substantial progress has been made by Gras [19] [16],[18],[17],[20] and Maire and Rougnant [32] investigated its isotypic components.

For fixed p, the general expectation is that among all real quadratic fields, the p-rational ones greatly outnumber the non p-rational ones (see Section 4.2.3 of [17]). A density type theorem of Byeon [6, Theorem 1.1] shows that for $p > 3$

$$\#\{K \text{ is real quadratic} \,|\, 0 < D_K < X, \text{ and } K \text{ is } p\text{-rational}\} \gg \frac{\sqrt{X}}{\log(X)}$$

Date: October 18, 2026.

Thanks to Jie Yang and Preston Wake for reading the draft of the paper.

(see also Ono [41]). On the other hand, it is expected that for a fixed number field K, the primes p such that K is non p-rational are rare (or possibly finite [18]). Assuming the generalized *abc*-conjecture, Maire and Rougnant [31] proved that if K is a real quadratic field or an imaginary S_3-extension of $\mathbb{Q}$, then there exists a constant $c_K > 0$ such that

$$\#\{p \leq X : K \text{ is } p\text{-rational}\} \geq c_K \log X$$

for X sufficiently large, see [30] for a similar result. For a fixed real quadratic field K, it is generally difficult to find a particular p such that K is non p-rational. However, if we fix p, it is easy to construct an infinite family of non p-rational real quadratic fields [20],[17]. Our Theorem 3.2 generalizes [17]. One can also construct a family of real quadratic fields by varying p. For example, $\mathbb{Q}(\sqrt{p(p+2)})$ is p-rational for odd primes $p > 5$ (see [17][2] for this kind of result).

Let $|\cdot|_\infty : \mathbb{R} \to \mathbb{R}^+$ be the usual absolute value.

Theorem 1.1. *Let $r \geq 2, m$ be positive integers, p be an odd prime, and $\gcd(p, m) = 1$. Denote $K = \mathbb{Q}(\sqrt{m^2p^{2r} + 1})$, and assume that*

$$|m|_\infty \leq \left| \frac{(1 + \binom{p^{r-1}}{2})p^{p^{r-1}-r}}{2^{p^{r-1}}} \right|_\infty$$

Then K is a non p-rational field.

This is Theorem 3.2 in Section 3. We also prove that, for a fixed p, this gives an infinite family of non p-rational real quadratic fields as $r \to \infty$. These fields were studied by Gras [17, Section 4.3] under the assumption that $m^2p^{2r} + 1$ is squarefree. We do not make this assumption. Gras assumes that $m^2p^{2r} + 1$ is squarefree, so the explicit Pell-type unit is the fundamental unit and its p-adic regulator can be computed directly. Our method removes the squarefreeness assumption: the explicit unit need not be fundamental, so we instead control its relation with the true fundamental unit and prove the required congruence for that unit. Thus, Gras obtains sharper quantitative regulator estimates, while our argument is designed to handle the non-squarefree case.

1.2. **Iwasawa Invariants and Greenberg's Conjecture.** Let p be an odd prime, K a number field, and let ζ_{p^n} be a primitive p^n-th root of unity. Then $\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}$ has a unique degree p^n sub-extension of $\mathbb{Q}$ denoted as $\mathbb{Q}_n$. Put $\mathbb{Q}_\infty = \bigcup_n \mathbb{Q}_n$ and $K_\infty = K\mathbb{Q}_\infty$. Then K_∞/K is a $\mathbb{Z}_p$-extension of K which we call the cyclotomic $\mathbb{Z}_p$-extension of K. We write K_n to be the n-th layer of the $\mathbb{Z}_p$-extension of K_∞/K.

Let A_n be the p primary part of the class group of K_n. Then Iwasawa proved [23] that there are constants $\mu, \lambda, \nu \in \mathbb{Z}$ for all sufficiently large n with

$$|A_n| = p^{\mu p^n + \lambda n + \nu}.$$

The constants λ, μ, and ν are called the Iwasawa invariants for K_∞/K. We may also write them as $\lambda_p(K_\infty/K)$, $\mu_p(K_\infty/K)$, and $\nu_p(K_\infty/K)$ when p, K and K_∞ are not clear from context.

When $K/\mathbb{Q}$ is abelian, Ferrero and Washington [10] showed that $\mu = 0$ for the cyclotomic $\mathbb{Z}_p$-extension of K, and Iwasawa conjectured that this should hold for any number field. On the other hand, much less is known about the λ invariant for the cyclotomic $\mathbb{Z}_p$-extension of K. In fact, the cyclotomic μ-invariant and

λ-invariant are thought to be zero for any totally real number field. This is known as Greenberg's conjecture [21].

To find evidence for Greenberg's conjecture, one may try to construct an infinite family of real quadratic fields K where $\lambda_p = 0$, for a fixed prime p. By a well-known theorem of Iwasawa [46, Prop 13.22], if p is inert in $K/\mathbb{Q}$, totally ramified in K_∞/K, and doesn't divide the class number h_K of K, then $\lambda = 0$. Therefore, one may try to find infinitely many fields such that p doesn't split and $p \nmid h_K$. This has been done by Ono [41] for $3 < p < 5000$, Ozaki and Taya [42] and Fukuda and Komatsu [11] when $p = 2$, as well as Horie and Nakagawa [39] when $p = 3$. These authors also studied the case when p splits, for $p = 2$ and $p = 3$ respectively. Kraft [29] has found a relation between the λ-invariants of certain imaginary and real quadratic fields when $p = 3$, which gives an infinite family of real quadratic fields with vanishing λ-invariant by Corollary 1.3 of Ito [22].

Recall that a prime p is called Wieferich prime if $p^2 \mid (2^{p-1} - 1)$.

Theorem 1.2. *Let $p \geq 3$ be a non-Wieferich prime and $r \geq 2$, and write $K = \mathbb{Q}(\sqrt{p^{2r} + 1})$. Assume that p doesn't divide the class number of K. Then the Iwasawa invariants μ and λ are zero for the cyclotomic $\mathbb{Z}_p$-extension of K.*

This is Theorem 4.4 in Section 4. We also prove that the fields $\mathbb{Q}(\sqrt{p^{2r} + 1})$ are distinct for distinct values of r. We expect that, for a fixed p, there are infinitely many r such that p doesn't divide the class number of $\mathbb{Q}(\sqrt{p^{2r} + 1})$, and hence an infinite family satisfying Greenberg's conjecture.

Remark 1.3. *There are other numerical criterion to conclude fields $K = \mathbb{Q}(\sqrt{p^{2r} + 1})$ satisfying Greenberg's conjecture. In the paper, we apply the numerical criterion of Fukuda and Komatsu [12], formulated in terms of the invariants n_1 and n_2, (see the definition in Section 4), to the fields $K = \mathbb{Q}(\sqrt{p^{2r} + 1})$. We note that other numerical criteria involving n_1 and n_2 have also been developed by Fukuda, Komatsu, and others; see, for example, [13, 14]. These alternative criteria may allow one to replace the class number condition in our theorem by different arithmetic hypotheses.*

1.3. **Structure of the Paper.** In Section 2, we study some general properties of the field $K = \mathbb{Q}(\sqrt{m^2p^{2r} + 1})$. In Section 3, we study the p-rationality of K. In Section 4, we study Greenberg's conjecture for K.

2. Construction of a Family of Real Quadratic Fields

In this section, we first study the basic properties of the real quadratic field $\mathbb{Q}(\sqrt{m^2p^{2r} + 1})$. Here m, r are positive integers and p is an odd prime which is prime to m. Let ε be the fundamental unit of $\mathbb{Q}(\sqrt{m^2p^{2r} + 1})$. Our focus throughout this paper will be on the following congruence

$$\varepsilon^{p-1} \equiv 1 \pmod{p^2}$$

which may or may not hold for a given arbitrary real quadratic field. This congruence appears as a key step in the numerical criterion to determine non p-rationality, and whether the Iwasawa invariants $\mu = \lambda = 0$. In the next section, we will use the results of this section to construct a family of real quadratic fields that are not p-rational. It is also a family of real quadratic fields whose Iwasawa invariant $\mu = \lambda = 0$ with a further assumption on the class number.

We first prepare some easy lemmas which we will need later on.

Lemma 2.1. *Let p be an odd prime and let $\varepsilon \in \mathbb{Z}_p^*$. Suppose that $t = \pm\varepsilon^k$ for some integer k prime to p. Then*

$$\varepsilon^{p-1} \equiv 1 \pmod{p^2\mathbb{Z}_p} \iff t^{p-1} \equiv 1 \pmod{p^2\mathbb{Z}_p}.$$

Proof. Set

$$U_1 = 1 + p\mathbb{Z}_p, \qquad U_2 = 1 + p^2\mathbb{Z}_p.$$

Since $\varepsilon^{p-1} \in U_1$ and p is odd, we have

$$t^{p-1} = (\pm\varepsilon^k)^{p-1} = (\varepsilon^{p-1})^k.$$

The quotient U_1/U_2 is a group of order p. Since $(k, p) = 1$, the k-th power map is an automorphism of U_1/U_2. Hence

$$(\varepsilon^{p-1})^k \in U_2 \iff \varepsilon^{p-1} \in U_2,$$

which is precisely the desired equivalence. □

Lemma 2.2. *Let D be a positive square-free integer and $K = \mathbb{Q}(\sqrt{D})$. Let t be a unit in $\mathcal{O}_K$. Assume that the odd prime p splits in K as $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. Then*

$$t^{p-1} \equiv 1 \pmod{\mathfrak{p}^2} \iff t^{p-1} \equiv 1 \pmod{\bar{\mathfrak{p}}^2} \iff t^{p-1} \equiv 1 \pmod{p^2\mathcal{O}_K}.$$

Proof. Let $\bar{t}$ be the Galois conjugate of t. Then $t^{p-1}\bar{t}^{p-1} = 1$, since t is a unit. Now,

$$\begin{aligned} t^{p-1} \equiv 1 \pmod{\mathfrak{p}^2} &\iff \bar{t}^{p-1} \equiv 1 \pmod{\bar{\mathfrak{p}}^2} \\ &\iff t^{p-1}\bar{t}^{p-1} \equiv t^{p-1} \pmod{\bar{\mathfrak{p}}^2} \\ &\iff 1 \equiv t^{p-1} \pmod{\bar{\mathfrak{p}}^2}. \end{aligned}$$

The last congruence comes from the fact that $t^{p-1} - 1 \in \mathfrak{p}^2 \cap \bar{\mathfrak{p}}^2 = p^2\mathcal{O}_K$. □

Remark 2.3. *We can embed K into $\mathbb{Q}_p$ by localization at prime $\mathfrak{p}$ or $\bar{\mathfrak{p}}$. The first congruence tells us that $t^{p-1} \equiv 1 \pmod{p^2\mathbb{Z}_p}$ doesn't depend on the choice of embedding. Later, we will write $t^{p-1} \equiv 1 \pmod{p^2}$ for simplicity. One can understand it as $t^{p-1} \equiv 1 \pmod{p^2\mathbb{Z}_p}$ by embedding K into $\mathbb{Q}_p$ or one can understand it as $t^{p-1} \equiv 1 \pmod{p^2\mathcal{O}_K}$. It doesn't matter since they are all equivalent.*

The proof of the following lemma is inspired by the proof of Theorem 3.4 of [5].

Lemma 2.4. *Let D be a positive square-free integer and $K = \mathbb{Q}(\sqrt{D})$. Assume that $p > 2$ splits in K. Let $t = a + b\sqrt{D}$ be a unit in $\mathcal{O}_K$, where $a, b \in \frac{1}{2}\mathbb{Z}$. Let* Nrm *denote the norm map from K to $\mathbb{Q}$. Assume that* $\mathrm{Nrm}(t) = -1$ *and $p \mid a$. Then*

$$t^{p-1} \equiv 1 \pmod{p^2} \iff a \equiv 0 \pmod{p^2}.$$

Proof. Let $\bar{t} = a - b\sqrt{D}$ be the Galois conjugates of t. Define the generalized Fibonacci sequence $\{F_n\}_n$ as

$$F_{n+2} = (t + \bar{t})F_{n+1} - \mathrm{Nrm}(t)F_n = 2aF_{n+1} + F_n$$

and $F_0 = 0$ and $F_1 = 1$. The Binet formula [28] tells us

$$F_n = \frac{t^n - \bar{t}^n}{t - \bar{t}} \text{ for any } n \geq 1.$$

Computing further into the sequence, we have $F_2 = 2a, F_3 = 4a^2 + 1, F_4 = 8a^3 + 4a$, and $F_5 = 16a^4 + 12a^2 + 1$. By induction, we have

$$F_{2n} \equiv 2na \pmod{a^2} \qquad \text{and} \qquad F_{2n-1} \equiv 1 \pmod{a^2}$$

and since we assumed that $p \mid a$, we have

$$F_{p-1} \equiv (p-1)a \pmod{p^2}.$$

Hence,

$$F_{p-1} \equiv 0 \pmod{p^2} \iff p^2 \mid a.$$

On the other hand, the Binet formula tells us

$$(t - \bar{t})F_{p-1} = t^{p-1} - \bar{t}^{p-1} = t^{1-p}(t^{p-1} - 1)(t^{p-1} + 1).$$

Since $-1 = t\bar{t} = a^2 - b^2D$, and $p \mid a$, we have $p \nmid b$ and $p \nmid (t - \bar{t})$. Since $p \nmid t^{1-p}(t^{p-1} + 1)$, we have

$$t^{p-1} \equiv 1 \pmod{p^2} \iff F_{p-1} \equiv 0 \pmod{p^2}.$$

□

Lemma 2.5. *Let $K = \mathbb{Q}(\sqrt{m^2p^{2r} + 1})$ where r, m are positive integers and p is an odd prime with $\gcd(p, m) = 1$. Then p splits in the real quadratic field K.*

Proof. Suppose $m^2p^{2r} + 1 = b^2D$, where D is a square-free integer and b is a positive integer. We have p splits in $K = \mathbb{Q}(\sqrt{D})$ if and only if the Legendre symbol $(\frac{D}{p}) = 1$. Notice that

$$\left(\frac{D}{p}\right) = \left(\frac{b^2D}{p}\right) = \left(\frac{m^2p^{2r} + 1}{p}\right) = \left(\frac{1}{p}\right) = 1.$$

□

Let $|\cdot|_\infty$ denote the usual absolute value on $\mathbb{R}$.

Theorem 2.6. *Let $K = \mathbb{Q}(\sqrt{m^2p^{2r} + 1})$ where $r \geq 2$, m are positive integers and p is an odd prime with $\gcd(p, m) = 1$. Let ε be the fundamental unit of K. Assume that*

$$|m|_\infty \leq \left| \frac{(1 + \binom{p^{r-1}}{2})p^{p^{r-1}-r}}{2^{p^{r-1}}} \right|_\infty$$

Then

$$\varepsilon^{p-1} \equiv 1 \pmod{p^2}.$$

Proof. Suppose $m^2p^{2r}+1=b^2D$, where D is a square-free integer and b is a positive integer. Write $t:=mp^r-b\sqrt{D}$. Then $\mathrm{Nrm}(t)=(mp^r-b\sqrt{D})(mp^r+b\sqrt{D})=-1$. By Lemma 2.4, we know that $t^{p-1}\equiv 1 \pmod{p^2}$. If $t=mp^r-b\sqrt{D}=\pm\varepsilon^k$ for some integer k prime to p, then the conclusion holds by lemma 2.1.

Now assume $t=mp^r-b\sqrt{D}=\pm\varepsilon^{p^lk}$ for some integer k prime to p and $l\geq 1$. Let $x+y\sqrt{D}:=\varepsilon^k$, where $x,y\in\frac{1}{2}\mathbb{Z}$.

By definition,

$$-1=(\pm t)(\pm\bar{t})=(x+y\sqrt{D})^{p^l}(x-y\sqrt{D})^{p^l}.$$

Hence,

$$(x+y\sqrt{D})(x-y\sqrt{D})=-1.$$

The norm $\mathrm{Nrm}(x+y\sqrt{D})=-1$.

We have

$$\begin{aligned}\pm(mp^r-b\sqrt{D}) =&(x+y\sqrt{D})^{p^l}\\ =&x^{p^l}+\binom{p^l}{1}x^{p^l-1}y\sqrt{D}+\binom{p^l}{2}x^{p^l-2}(y\sqrt{D})^2+\binom{p^l}{3}x^{p^l-3}(y\sqrt{D})^3\\ &+\cdots+\binom{p^l}{p^l-1}x(y\sqrt{D})^{p^l-1}+(y\sqrt{D})^{p^l}.\end{aligned}\tag{1}$$

Then

$$\pm mp^r=x^{p^l}+\binom{p^l}{2}x^{p^l-2}(y\sqrt{D})^2+\cdots+\binom{p^l}{p^l-1}x(y\sqrt{D})^{p^l-1}.\tag{2}$$

We know $\binom{p^l}{k}\equiv 0 \pmod{p}$ for $1<k<p^l$. So, (2) implies

$$0\equiv x^{p^l} \pmod{p}.$$

Therefore $p\mid x$.

Comparing the coefficient of $\sqrt{D}$ in equation (1), we have

$$\pm b=\binom{p^l}{1}x^{p^l-1}y+\binom{p^l}{3}x^{p^l-3}y^3D+\cdots+y^{p^l}D^{\frac{p^l-1}{2}}.$$

Reducing both sides modulo p, we have

$$\pm b\equiv y^{p^l}D^{\frac{p^l-1}{2}} \pmod{p}.$$

Since $p\nmid b$ and $p\nmid D$, we get $p\nmid y$.

Now, assume $p^2\nmid x$. Hence $v_p(x)=1$ where v_p is the p-adic valuation. By the standard valuation formula,

$$v_p(\binom{p^l}{i})=l-v_p(i)\qquad(1\leq i\leq p^l)$$

(see, for example, [8, §11.5, p. 353], [1]). Hence, for $i\geq 1$,

$$v_p\left(\binom{p^l}{i}x^i(y\sqrt{D})^{p^l-i}\right)=l-v_p(i)+i\geq l+1$$

with equality holding if and only if $i=1$, since we have assumed p is an odd prime. We have

$$r=v_p(\pm mp^r)=v_p(\sum_{odd\,i}\binom{p^l}{i}x^i(y\sqrt{D})^{p^l-i})=l+1.$$

Now, taking the real absolute value $|\cdot|_\infty$ of both side of equation 2,

$$\begin{aligned}|mp^r|_\infty &= |x^{p^l} + \binom{p^l}{2}x^{p^l-2}(y\sqrt{D})^2 + \cdots + \binom{p^l}{p^l-1}x(y\sqrt{D})^{p^l-1}|_\infty \\ &> |x^{p^l} + \binom{p^l}{2}x^{p^l-2}(y^2D)|_\infty \\ &= |x^{p^l} + \binom{p^l}{2}x^{p^l-2}(x^2+1)|_\infty \\ &> |(1+\binom{p^l}{2})x^{p^l}|_\infty.\end{aligned}$$

We know $x \in \frac{1}{2}\mathbb{Z}$, $p \mid x$, and $x \neq 0$. Hence $|x|_\infty \geq \frac{p}{2}$. Since $r = l+1$

$$|m|_\infty > \left|\frac{(1+\binom{p^l}{2})x^{p^l}}{p^r}\right|_\infty \geq \left|\frac{(1+\binom{p^{r-1}}{2})p^{p^{r-1}-r}}{2^{p^{r-1}}}\right|_\infty$$

which contradicts our assumption on m. Hence, we must have $p^2|x$.

Now, we know $p^2 \mid x$ and the norm $\mathrm{Nrm}(x+y\sqrt{D}) = -1$. By Lemma 2.4, we know $(x+y\sqrt{D})^{p-1} \equiv 1 \pmod{p^2}$. Then by Lemma 2.1, we have $\varepsilon^{p-1} \equiv 1 \pmod{p^2}$. □

Remark 2.7. *The condition on the upper bound of $|m|_\infty$ is only used in the case that $t = mp^r - b\sqrt{D}$ is the pth-power of a unit. In our SageMath experiments, for a fixed prime p and varying m and r, we found that in most cases $t = mp^r - b\sqrt{D}$ is not the p-th power of a unit. When m is odd,*

$$b^2D = 1 + m^2p^{2r} \equiv 1 + 1 = 2 \pmod 4$$

implies that $D \equiv 2 \mod 4$, and we can assume $x \in \mathbb{Z}$. This allows us to further relax the upper bound. However, the upper bound is enough for our purposes since we take $m = 1$ in a later section.

We take $m = 1$ in the next lemma. It is a generalization of Exercise 8.3.3 in [38].

Lemma 2.8. *Let $p^{2r} + 1 = b^2D$, where D is a square-free integer, $r \geq 2, b$ are positive integers, and $p \geq 3$ is an odd prime. Let $K = \mathbb{Q}(\sqrt{D})$. Then $p^r + b\sqrt{D}$ is a fundamental unit for K.*

Proof. Note that $D \equiv 2 \pmod 4$, so the ring of integers of $\mathbb{Q}(\sqrt{D})$ is $\mathbb{Z}[\sqrt{D}]$. Now, we know $t = p^r + b\sqrt{D}$ is a unit. Let $\varepsilon_D = x + y\sqrt{D}$ be the fundamental unit (without loss of generality we may take $x, y > 0$), and suppose $t = \varepsilon_D^k$ for some $k \in \mathbb{Z}^+$. We will prove that $k = 1$.

Assume k is even. Then

$$-1 = \mathrm{Nrm}(p^r + b\sqrt{D}) = \mathrm{Nrm}(\varepsilon_D^k) = (\pm 1)^k = 1$$

which is a contradiction. This also implies that $\mathrm{Nrm}(\varepsilon_D) = -1$.

Now, assume that k is odd and q is an odd prime such that $q \mid k$. Write $v + w\sqrt{D} = \varepsilon_D^{k/q}$. Then $t = (v + w\sqrt{D})^q$, and

$$p^r = \sum_{i=0}^{(q-1)/2} \binom{q}{2i} w^{2i} D^i v^{q-2i} = vu \tag{3}$$

where

$$u = \sum_{i=0}^{(q-1)/2} \binom{q}{2i} w^{2i} D^i v^{q-2i-1} \geq \binom{q}{0} w^0 D^0 v^{q-0-1} = v^{q-1}. \tag{4}$$

Notice $v^2 - w^2 D = \mathrm{Nrm}(\varepsilon_D^{k/q}) = -1$ implies that $\gcd(v, w) = \gcd(v, D) = 1$. By equation (4), we have $\gcd(v, u) = \gcd(v, \binom{q}{q-1} w^{q-1} D^{(q-1)/2}) = \gcd(v, q)$.

Suppose $\gcd(v, q) = 1$. Now, $p^r = uv$, so it must be that $v = 1$ and $u = p^r$ since $u > 1$. But then $v^2 - w^2 D = -1$ so that $w^2 D = 2$ which implies $D = 2$ and $w = 1$. We have $p^{2r} + 1 = 2b^2$. Theorem 1.1 of [3] classifies all integer solutions to the equation $x^r + y^r = 2z^2$. As a consequence, the equation $p^{2r} + 1 = 2b^2$ has no integer solutions of the desired form when $p \geq 3$.

Suppose $\gcd(v, q) = q$. Since $p^r = uv$, it follows that $v = p^l$, and $u = p^{r-l}$ for some integer $l \geq 1$. In particular, we must have $q = p$, and moreover $\gcd(p, w) = \gcd(v, w) = 1, \gcd(p, D) = \gcd(v, D) = 1$. Applying the same trick as in the proof of Theorem 2.6. When $0 \leq i \leq \frac{p-1}{2}$, we have

$$\begin{aligned} v_p\left(\binom{p}{2i} w^{2i} D^i v^{p-2i}\right) &= v_p\left(\binom{p}{2i}\right) + v_p(w^{2i}) + v_p(D^i) + v_p(v^{p-2i}) \\ &= 1 - v_p(2i) + 0 + 0 + l(p - 2i) \\ &= 1 + l(p - 2i). \end{aligned}$$

The minimum occurs precisely when $i = \frac{p-1}{2}$. Taking p-adic valuations on both sides of equation (3), we obtain

$$r = 1 + l\big(p - 2 \cdot \tfrac{p-1}{2}\big) = 1 + l,$$

which implies $v = p^{r-1}$ and $u = p$. However, this contradicts the condition $u \geq v^{p-1}$.

□

Lemma 2.9. *For $i = 1, 2$, assume $r_i \geq 2$ and $p \geq 3$ is an odd prime. We have $\mathbb{Q}(\sqrt{p^{2r_1} + 1}) = \mathbb{Q}(\sqrt{p^{2r_2} + 1})$ if and only if $r_1 = r_2$.*

Proof. Assume that $p^{2r_i} + 1 = b_i^2 D_{r_i}$, where D_{r_i} are a square-free integer and b_i are positive integers. By lemma 2.8, the fundamental unit of $\mathbb{Q}(\sqrt{D_{r_1}})$ is $p^{r_1} + b_1\sqrt{D_{r_1}}$ and the fundamental unit of $\mathbb{Q}(\sqrt{D_{r_2}})$ is $p^{r_2} + b_2\sqrt{D_{r_2}}$. Hence $\mathbb{Q}(\sqrt{D_{r_1}}) = \mathbb{Q}(\sqrt{D_{r_2}})$ implies that

$$p^{r_1} + b_1\sqrt{D_{r_1}} = \pm(p^{r_2} + b_2\sqrt{D_{r_2}})^{\pm 1}.$$

We know that $(p^{r_2} + b_2\sqrt{D_{r_2}})^{-1} = -p^{r_2} + b_2\sqrt{D_{r_2}}$. Hence we must have $r_1 = r_2$. □

By lemma 2.8 and lemma 2.9, for a fixed odd prime p, the family of real quadratic fields $\{\mathbb{Q}(\sqrt{p^{2r} + 1}) | r \in \mathbb{N}, r \geq 2\}$ is an infinite family. Next, we will consider the p-rationality and Iwasawa invariants μ, λ for $\mathbb{Q}(\sqrt{m^2 p^{2r} + 1})$ in the following sections.

3. p-RATIONALITY

We recall the notion of a p-rational number field, see exposition [26] [36, 37, 40]; see also [15] for further developments and [34, Section 3.3.2] for equivalent formulations in the real quadratic case.

Let K be a number field and p an odd prime. Let L be the maximal abelian pro-p extension of K unramified outside p. Assuming Leopoldt's conjecture for K, if K has r_2 pairs of complex embeddings, then

$$\mathrm{Gal}(L/K) \cong \mathbb{Z}_p^{r_2+1} \times \mathcal{T}_K,$$

where $\mathcal{T}_K$ is a finite abelian p-group. The field K is called p-rational if $\mathcal{T}_K = 0$. The order of $\mathcal{T}_K$ is related to special values of p-adic L-functions; we will use the following theorem of Coates [7, Appendix].

Theorem 3.1 (Coates)**.** *Let K be a totally real field and p be an odd prime. Assume Leopoldt's conjecture holds for K. Then $\#\mathcal{T}_K$ has the same p-adic valuation as*

$$\frac{w_1(K(\mu_p))h_K R_p(K) \prod_{\mathfrak{p}|p}(1-(\mathrm{Nrm}\,\mathfrak{p})^{-1})}{\sqrt{\Delta_{K/\mathbb{Q}}}}$$

Here μ_p is the group of p-th roots of unity, $w_1(K(\mu_p))$ is the number of roots of unity of $K(\mu_p)$, h_K is the class number of K, $R_p(K)$ is the p-adic regulator of K, $\mathrm{Nrm}\,\mathfrak{p}$ is the absolute norm of $\mathfrak{p}$, and $\Delta_{K/\mathbb{Q}}$ is the discriminant of K.

Theorem 3.2. *Let $r \geq 2, m$ be positive integers, p be an odd prime, and $\gcd(p,m) = 1$. Denote $K = \mathbb{Q}(\sqrt{m^2p^{2r}+1})$, and assume that*

$$|m|_\infty \leq \left| \frac{(1+\binom{p^{r-1}}{2})p^{p^{r-1}-r}}{2^{p^{r-1}}} \right|_\infty .$$

Then K is a non p-rational field.

Proof. We will use Theorem 3.1 of Coates. Since K is a real quadratic field, $w_1(K(\mu_p)) = 2p$. By Lemma 2.5, p splits in K. Hence, $\prod_{\mathfrak{p}|p}(1-(\mathrm{Nrm}\,\mathfrak{p})^{-1}) = (p-1)^2/p^2$. Let ε_D be the fundamental unit of K. Notice that the p-adic regulator $R_p(K) = \log_p(\varepsilon_D) \equiv 0 \pmod{p^2} \iff \varepsilon_D^{p-1} \equiv 1 \pmod{p^2}$. By Theorem 2.6, we know that $v_p(R_p(K)) \geq 2$. Since $\gcd(p, m^2p^{2r}+1) = 1$, the discriminant $\Delta_{K/\mathbb{Q}}$ is prime to p. Putting everything together,

$$\begin{aligned} v_p\left(\omega_1(K(\mu_p))\prod_{\mathfrak{p}|p}(1-\mathrm{Nrm}(\mathfrak{p})^{-1})\frac{R_p(K)h_K}{\sqrt{\Delta_{K/\mathbb{Q}}}}\right) =& v_p(\omega_1(K(\mu_p))) + v_p\left(\prod_{\mathfrak{p}|p}(1-\mathrm{Nrm}(\mathfrak{p})^{-1})\right) \\ &+ v_p(R_p(K)) + v_p(h_K) - v_p\left(\sqrt{\Delta_{K/\mathbb{Q}}}\right) \\ \geq& 1 - 2 + 2 + v_p(h_K) - 0 \\ \geq& 1. \end{aligned}$$

Hence, $v_p(\#\mathcal{T}_K) \geq 1$ by Theorem 3.1, and therefore the real quadratic field K is a non p-rational field.

□

Corollary 3.3. *For a fixed odd prime p, there is an infinite family of non p-rational real quadratic fields.*

Proof. By Theorem 3.2, the members of the following set are non p-rational real quadratic fields.

$$\left\{ \mathbb{Q}(\sqrt{m^2p^{2r}+1}) \,\middle|\, r \geq 2, m \in \mathbb{Z}^+, \gcd(p,m)=1, |m|_\infty \leq \left| \frac{(1+\binom{p^{r-1}}{2}))p^{p^{r-1}-r}}{2^{p^{r-1}}} \right|_\infty \right\}$$

This set contains the following subset,

$$\{\mathbb{Q}(\sqrt{p^{2r}+1}) \,|\, r \geq 2\}.$$

By Lemmas 2.8 and 2.9, this subset is an infinite set. Hence, we have an infinite family of non p-rational real quadratic fields. □

The family of Corollary 3.3 overlaps with some families found in [20] and [17].

4. Iwasawa Invariants

In this section, we will consider the Iwasawa invariants μ and λ of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}(\sqrt{p^{2r}+1})$. In [21], Greenberg conjectured that the Iwasawa invariant $\mu = \lambda = 0$ for the cyclotomic $\mathbb{Z}_p$-extension for any totally real field. To test the conjecture, other authors have developed numerical criterion to determine when $\mu = \lambda = 0$ for real quadratic fields (see for example [24][13][12][14][45][33]). It is then natural to use these criteria to construct infinite families of real quadratic fields such that Greenberg's conjecture holds (see for example [35][42][11][39][29]). In this section, we first recall a numerical criterion developed by Fukuda and Komatsu [12]. Then we apply the criterion to the real quadratic field $\mathbb{Q}(\sqrt{p^{2r}+1})$.

Let K be any real quadratic field and p be an odd prime. Let h_K be the class number of K. Assume that p splits in K as $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. Let α be a generator of the principal ideal $\bar{\mathfrak{p}}^{h_K}$. Let ε_K be the fundamental unit of K. Define the integers n_1 and n_2 such that

$$\alpha^{p-1} \equiv 1 \pmod{\mathfrak{p}^{n_1}} \quad \text{and} \quad \alpha^{p-1} \not\equiv 1 \pmod{\mathfrak{p}^{n_1+1}}$$

$$\varepsilon_K^{p-1} \equiv 1 \pmod{\mathfrak{p}^{n_2}} \quad \text{and} \quad \varepsilon_K^{p-1} \not\equiv 1 \pmod{\mathfrak{p}^{n_2+1}}.$$

The value of n_1 does not depend on the choice of α and is uniquely determined under the condition $n_1 \leq n_2$. Fukuda and Komatsu, among other authors, have developed a series of criterion in terms of invariant n_1, n_2 to check Greenberg's conjecture for real quadratic fields [13][12][14]. Here we only recall one criterion from [12].

Let $K = K_0 \subset K_1 \subset K_2 \cdots \subset K_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of K. Let A_n be the p-primary part of the class group of K_n. Let D_n be the subgroup of A_n generated by the prime ideals above p.

Theorem 4.1 (Fukuda and Komatsu [12])**.** *Let K be a real quadratic field and p an odd prime which splits in $K/\mathbb{Q}$. Assume that*

(a) $n_1 = 1$
(b) $A_0 = D_0$

Then, for $n \geq n_2 - 1$, we have $|A_n| = |D_n| = |D_0| \cdot p^{n_2-1}$.

Let $p^{2r}+1=b^2D$, where D is a square-free integer, $r\geq 2, b$ are positive integers, and $p\geq 3$ is an odd prime. Let $K=\mathbb{Q}(\sqrt{D})$. By lemma 2.5, we know p splits in K, say $p\mathcal{O}_K=\mathfrak{p}\bar{\mathfrak{p}}$. Notice that we can factor $p^{2r}=b^2D-1=(b\sqrt{D}+1)(b\sqrt{D}-1)$ in $\mathcal{O}_K$. Hence, we can take $\mathfrak{p}^{2r}=(b\sqrt{D}-1)$ and $\bar{\mathfrak{p}}^{2r}=(b\sqrt{D}+1)$. Let ε_D be the fundamental unit of K. Then by Theorem 2.6, we know

$$\varepsilon_D^{p-1}\equiv 1 \pmod{p^2}$$

and therefore $n_2\geq 2$. In fact, we can further determine the explicit value of n_2.

Lemma 4.2. *Keeping the same setup as before, we have $n_2=r$.*

Proof. By Lemma 2.8, we can take $p^r+b\sqrt{D}$ as the fundamental unit of K. Notice that $\mathfrak{p}^{2r}=(b\sqrt{D}-1)$ tells us $b\sqrt{D}\equiv 1 \pmod{\mathfrak{p}^{2r}}$. Since $r\geq 2$, we have $2r>r+1>r$. Therefore,

$$(p^r+b\sqrt{D})^{p-1}\equiv (p^r+1)^{p-1}\equiv 1^{p-1}=1 \pmod{\mathfrak{p}^r}$$

but

$$(p^r+b\sqrt{D})^{p-1}\equiv (p^r+1)^{p-1}\equiv \sum_{i=0}^{p-1}\binom{p-1}{i}p^{ri}\equiv 1+(p-1)p^r\not\equiv 1 \pmod{\mathfrak{p}^{r+1}}.$$

□

Lemma 4.3. *Keeping the same setup as before, we have $(b\sqrt{D}+1)^{p-1}\equiv 2^{p-1} \pmod{\mathfrak{p}^2}$.*

Proof. Since we have $b\sqrt{D}\equiv 1 \pmod{\mathfrak{p}^{2r}}$,

$$(b\sqrt{D}+1)^{p-1}\equiv (1+1)^{p-1}=2^{p-1} \pmod{\mathfrak{p}^2}.$$

□

Recall that a prime number p is called a Wieferich prime if $p^2\mid (2^{p-1}-1)$. These primes are thought to be sparse (the only known Wieferich primes are 1093 and 3511 [47]). Crandall, Dilcher, and Pomerance [9] proposed a heuristic about the probability for a prime p to be Wieferich and suggested that the number of Wieferich primes up to X should grow like $\log\log X$, and hence that there should be infinitely many such primes. On the other hand, Gras [16] proposed different probabilistic heuristics for Fermat quotients, suggesting that there may be only finitely many Wieferich primes p. At present, neither prediction is known to be correct, and the very slow growth of $\log\log X$ makes the available numerical evidence insufficient to distinguish clearly between these two possibilities. We also note that Silverman [44] has shown the infinitude of non-Wieferich primes under the assumption of the *abc*-conjecture. The relation between p-rationality and Wieferich-type congruences has also been studied by Böckle, Guiraud, Kalyanswamy, and Khare [4].

Theorem 4.4. *Let $p\geq 3$ be a non-Wieferich prime and $r\geq 2$, and write $K=\mathbb{Q}(\sqrt{p^{2r}+1})$. Assume that p doesn't divide the class number h_K. Then the Iwasawa invariants μ,λ are zero for the cyclotomic $\mathbb{Z}_p$-extension of K.*

Proof. Let s be the order of the class of $\bar{\mathfrak{p}}$ in the class group of K and $\bar{\mathfrak{p}}^s=(t)$ for some $t\in K^*$. Since $\bar{\mathfrak{p}}^{2r}=(b\sqrt{D}+1)$, then for some integer k_1,

$$b\sqrt{D}+1=\pm t^{2r/s}\varepsilon_K^{k_1}$$

By Lemma 4.2, $\varepsilon_K^{p-1} \equiv 1 \pmod{\mathfrak{p}^2}$, and by Lemma 4.3, $(b\sqrt{D}+1)^{p-1} \equiv 2^{p-1} \not\equiv 1 \pmod{\mathfrak{p}^2}$. Hence $t^{p-1} \not\equiv 1 \pmod{\mathfrak{p}^2}$. Let α be a generator of $\bar{\mathfrak{p}}^{h_K}$. Then for some integer k_2, we have

$$\alpha = \pm t^{h_K/s} \varepsilon_K^{k_2}$$

Since $\gcd(p, h_K) = 1$, by localizing K at $\mathfrak{p}$ we can use Lemma 2.1 to conclude that $\alpha^{p-1} \not\equiv 1 \pmod{\mathfrak{p}^2}$. Thus, $n_1 = 1$.

Since $\gcd(p, h_K) = 1$, we have $D_0 = A_0 = 0$. Therefore, by Theorem 4.1, the Iwasawa invariant μ, λ vanish for the cyclotomic $\mathbb{Z}_p$-extension of K. □

Corollary 4.5. *Fix a non-Wieferich prime p. Then Greenberg's conjecture holds for the members of the following set.*

$$\left\{ \mathbb{Q}(\sqrt{p^{2r}+1}) \,|\, r \geq 2, p \text{ doesn't divide the class number of } \mathbb{Q}(\sqrt{p^{2r}+1}) \right\}$$

The following conjecture is motivated by our work and our computational data also suggests it.

Conjecture 4.6. *For a fixed prime $p > 2$, there are infinitely many $r \in \mathbb{Z}^+$ such that p does not divide the class number of $\mathbb{Q}(\sqrt{p^{2r}+1})$.*

As noted above, other numerical criteria in terms of n_1 and n_2 are available [13, 14]. Our assumption that p does not divide the class number of K ensures that $A_0 = D_0$, allowing us to apply Theorem 4.1; this assumption could be weakened by assuming $A_0 = D_0$ directly or by using other numerical criteria.

References

[1] B. J. (https://math.stackexchange.com/users/12507/bruno-joyal). *Prime dividing the binomial coefficients*. Mathematics Stack Exchange. URL:https://math.stackexchange.com/q/51475 (version: 2013-02-18). eprint: `https://math.stackexchange.com/q/51475`.

[2] Y. Benmerieme and A. Movahhedi. "Multi-quadratic p-rational number fields". In: *Journal of Pure and Applied Algebra* 225.9 (2021), p. 106657.

[3] M. A. Bennett and C. M. Skinner. "Ternary Diophantine Equations via Galois Representations and Modular Forms". In: *Canadian Journal of Mathematics* 56.1 (2004), pp. 23–54.

[4] G. Böckle, D.-A. Guiraud, S. Kalyanswamy, and C. Khare. "Wieferich primes and a mod p Leopoldt conjecture". In: *Arithmetic Geometry*. Ed. by N. Fakhruddin, E. Ghate, A. Nair, C. S. Rajan, and S. Varma. Vol. 41. Tata Institute of Fundamental Research Studies in Mathematics. Mumbai: Tata Institute of Fundamental Research, 2024, pp. 21–64.

[5] Z. Bouazzaoui. *Fibonacci Sequences And Real Quadratic p-Rational Fields*. 2019. arXiv: `1902.04795 [math.NT]`.

[6] D. Byeon. "Indivisibility of Class Numbers and Iwasawa λ-Invariants of Real Quadratic Fields". In: *Compositio Mathematica* 126.3 (2001), pp. 249–256.

[7] J. Coates. "p-adic L-functions and Iwasawa's theory". In: *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*. Academic Press, London-New York, 1977, pp. 269–353.

[8] H. Cohen. *Number Theory, Volume II: Analytic and Modern Tools*. Vol. 240. Graduate Texts in Mathematics. Springer, 2007.

[9] R. Crandall, K. Dilcher, and C. Pomerance. "A search for Wieferich and Wilson primes". In: *Mathematics of Computation* 66.217 (1997), pp. 433–449.

[10] B. Ferrero and L. Washington. "The Iwasawa Invariant μ_p Vanishes for Abelian Number Fields". In: *Annals of Mathematics* (1979), pp. 377–395.

[11] T. Fukuda and K. Komatsu. "On the Iwasawa λ-Invariant of the Cyclotomic $\mathbb{Z}_2$-Extension of a Real Quadratic Field". In: *Tokyo J. Math* 28.1 (2005), pp. 259–264.

[12] T. Fukuda and K. Komatsu. "On $\mathbb{Z}_p$-extensions of real quadratic fields". In: *J. Math. Soc. Japan* 38.1 (1986), pp. 95–102.

[13] T. Fukuda and K. Komatsu. "On the λ invariants of $\mathbb{Z}_p$-extensions of real quadratic fields". In: *Journal of Number Theory* 23.2 (1986), pp. 238–242.

[14] T. Fukuda and H. Taya. "The Iwasawa λ-invariants of $\mathbb{Z}_p$-extensions of real quadratic fields". In: *Acta Arithmetica* 69 (1995), pp. 277–292.

[15] G. Gras. *Class Field Theory: From Theory to Practice*. Springer Monographs in Mathematics. Berlin: Springer-Verlag, 2003, pp. xiii+491.

[16] G. Gras. "Étude probabiliste des quotients de Fermat". In: *Functiones et Approximatio Commentarii Mathematici* 54.1 (2016), pp. 115–140.

[17] G. Gras. "Heuristics and conjectures in the direction of a p-adic Brauer–Siegel Theorem". In: *Mathematics of Computation* 88.318 (2019), pp. 1929–1965.

[18] G. Gras. "Les θ-régulateurs locaux d'un nombre algébrique: Conjectures p-adiques". In: *Canadian Journal of Mathematics* 68.3 (2016), pp. 571–624.

[19] G. Gras. "The p-adic Kummer–Leopoldt Constant—Normalized p-adic Regulator". In: *International Journal of Number Theory* 14.2 (2018), pp. 329–337.

[20] G. Gras. "Unlimited lists of quadratic integers of given norm application to some arithmetic properties". In: *Communications in Advanced Mathematical Sciences* (Sept. 2023).

[21] R. Greenberg. "On the Iwasawa invariants of totally real number fields". In: *Amer. J. Math.* 98.1 (1976), pp. 263–284.

[22] A. Ito. "On certain infinite families of imaginary quadratic fields whose Iwasawa λ invariant is equal to 1". In: *Acta Arithmetica* 168.4 (2015), pp. 301–339.

[23] K. Iwasawa. "On $\mathbb{Z}_l$-Extensions of Algebraic Number Fields". In: *Annals of Mathematics* 98.2 (1973), pp. 246–326.

[24] J.-F. Jaulent. "Note sur la conjecture de Greenberg". In: *J. Ramanujan Math. Soc.* 34.1 (2019), pp. 59–80.

[25] J.-F. Jaulent. "Sur l'indépendance ℓ-adique de nombres algébriques". In: *Journal of Number Theory* 20 (1985), pp. 149–158.

[26] J.-F. Jaulent and T. Nguyen Quang Do. "Corps p-réguliers, corps p-rationnels et ramification restreinte". In: *Journal de Théorie des Nombres de Bordeaux* 5 (1993), pp. 343–363.

[27] J.-F. Jaulent and O. Sauzet. "Pro-ℓ-extensions de corps de nombres ℓ-rationnels". In: *Journal of Number Theory* 65 (1997), pp. 240–267.

[28] D. Kalman and R. Mena. "The Fibonacci Numbers: Exposed". In: *Mathematics Magazine* 76.3 (2003), pp. 167–181.

[29] J. Kraft. "Class Numbers and Iwasawa Invariants of Quadratic Fields". In: *PROCEEDINGS OF THE AMERICAN MATHEMATICAL SOCIETY* 124.1 (1996), pp. 31–34.

[30] H. Li and D. Qiu. "On p-Rationality of Cubic and Quartic Number Fields". In: *International Journal of Number Theory* 22.5 (2026), pp. 1099–1110.

[31] C. Maire and M. Rougnant. "A note on p-rational fields and the *abc*-conjecture". In: *Proceedings of the American Mathematical Society* 148.8 (2020), pp. 3263–3271.

[32] C. Maire and M. Rougnant. "Composantes isotypiques de pro-p-extensions de corps de nombres et p-rationalité". In: *Publicationes Mathematicae Debrecen* 94.1–2 (2019), pp. 123–155.

[33] W. G. McCallum. "Greenberg's conjecture and units in multiple $\mathbb{Z}_p$-extensions". In: *Amer. J. Math.* 123.5 (2001), pp. 909–930.

[34] G. McConnell. *Some new infinite families of non-p-rational real quadratic fields*. 2024. arXiv: `2406.14632 [math.NT]`.

[35] Y. Mizusawa and Y. Saito. "On $\mathbb{Z}_2$-extensions of real quadratic fields with four odd ramified prime numbers". In: *The Ramanujan Journal* 70.1 (2026).

[36] A. Movahhedi. "Sur les p-extensions des corps p-rationnels". In: *Math. Nachr.* 149 (1990), pp. 163–176.

[37] A. Movahhedi and T. Nguyen Quang Do. "Sur l'arithmétique des corps de nombres p-rationnels". In: Progress in Mathematics 81 (1990). Ed. by C. Goldstein, pp. 155–200.

[38] M. R. Murty and J. Esmonde. *Problems in Algebraic Number Theory*. 2nd. Springer, 2005.

[39] J. Nakagawa and K. Horie. "Elliptic curves with no rational points". In: *Proc. Amer. Math. Soc.* 104.1 (1988), pp. 20–24.

[40] T. Nguyen-Quang-Do. "Sur la $\mathbb{Z}_p$-torsion de certains modules galoisiens". fr. In: *Annales de l'Institut Fourier* 36.2 (1986), pp. 27–46.

[41] K. Ono. "Indivisibility of Class Numbers of Real Quadratic Fields". In: *Compositio Mathematica* 119.1 (1999), pp. 1–11.

[42] M. Ozaki and H. Taya. "On the Iwasawa λ_2-invariants of certain families of real quadratic fields". In: *Manuscripta Mathematica* 94.4 (1997), pp. 437–444.

[43] I. R. Shafarevich. "Extensions à points de ramification donnés". In: *Publications Mathématiques de l'IHÉS* 18 (1963), pp. 71–92.

[44] J. H. Silverman. "Wieferich's criterion and the *abc*-conjecture". In: *J. Number Theory* 30.2 (1988), pp. 226–237.

[45] H. Taya. "On cyclotomic $\mathbf{Z}_p$-extensions of real quadratic fields". In: *Acta Arith.* 74.2 (1996), pp. 107–119.

[46] L. C. Washington. *Introduction to cyclotomic fields*. Second. Vol. 83. Graduate Texts in Mathematics. Springer-Verlag, New York, 1997, pp. xiv+487.

[47] Wikipedia contributors. *Wieferich prime — Wikipedia, The Free Encyclopedia*. [Online; accessed 7-July-2024]. 2024.

[48] K. Wingberg. "Freie Produktzerlegungen von Galoisgruppen und Iwasawa-Invarianten für p-Erweiterungen von $\mathbb{Q}$". In: *Journal für die reine und angewandte Mathematik* 341 (1983), pp. 111–129.

Email address: qipeikai@amms.ac.cn

Chinese Academy of Science, Beijing, China

Email address: mathewsonstokes@gmail.com

Randolph College, Lynchburg, Virginia, USA