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, 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 [FK86b] to show that if p does not divide the class number of K, then the Iwasawa invariants 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 $\mathrm{Gal}(L/F)$. We say F is p-rational if $\mathcal{T}_F$ vanishes. The concept of p-rationality comes from the ramification theory, [Mov90] [NM90][Ngu86]. Recall that Leopoldt's conjecture predicts that $\rho = r_2 + 1$, where $2r_2$ is the number of complex embeddings $F \hookrightarrow \mathbb{C}$.

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 [Gra19]). For instance, Byeon [Bye01, Theorem 1.1] shows that for $p > 3$

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

(see also Ono [Ono99]). It is also thought, that for a fixed real quadratic field K, there are only finitely many p such that K is non p-rational. 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 [Gra23],[Gra19]. Our theorem 3.2 generalizes [Gra19] and may overlap with [Gra23]. It is proved that there are infinitely many p-rational totally real fields for a given p [Sil88], under the hypothesis of the *abc*-conjecture. 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 (see [Gra19][Ben21] for this kind of result).

Let $|\cdot|_\infty$ be the absolute value of a real number.

Date: July 28, 2024.

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

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 proved that, for a fixed p, this gives a family of infinite many non p-rational real quadratic fields as $r \to \infty$. These fields were studied by Gras [Gra19, Section 4.3] under the assumption that $m^2p^{2r}+1$ is squarefree. We do not make this assumption.

1.2. **Iwasawa Invariants and Greenberg's Conjecture.** Let p be a prime, K a number field. Let ζ_{p^n} be the 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. Let K_n 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 [Iwa73] that there are constants $\mu, \lambda, \nu \in \mathbb{Z}$ for all sufficiently large $n \in \mathbb{Z}^+$

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

The constants λ, μ, and ν are called the Iwasawa invariants for K_∞/K. We 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 the text.

When $K/\mathbb{Q}$ is abelian, Ferrero and Washington [FW79] showed that μ_p is 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 [Gre76].

To test Greenberg's conjecture, for a fixed prime p one may try to find an infinite family of real quadratic fields K satisfying Greenberg's conjecture. By a well-known theorem of Iwasawa [Was97, 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 construct infinitely many fields such that p doesn't split and $p \nmid h_K$. This has been done by Ozaki and Taya [OT97] and Fukuda and Komatsu [FK05] when $p = 2$, as well as Horie and Nakagawa [NH88] when $p = 3$. These authors also studied the case when p splits, for $p = 2$ and $p = 3$ respectively. Kraft [Kra96] 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 Itoh [Ito12].

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, except for finitely many cases where $\mathbb{Q}(\sqrt{p^{2r}+1}) = \mathbb{Q}(\sqrt{2})$. 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. We don't know how to prove this, but there may be another approach, as we now explain.

We applied a numerical criterion developed by Fukuda and Komatsu [FK86b] to conclude $K = \mathbb{Q}(\sqrt{p^{2r}+1})$ satisfying Greenberg's conjecture in the theorem. The numerical criterion [FK86b] is in terms of invariants n_1, n_2. (See the definition in Section 4). Roughly speaking, we have $n_1 = 1$ and $n_2 = r$ for $K = \mathbb{Q}(\sqrt{p^{2r}+1})$. It is possible to apply other different kinds of numerical criterion in terms of invariants n_1, n_2 developed by Fukuda, Komatsu, and other authors [Fuk86][FK86a][FT95]. In this way, one may replace the condition on the class number with another condition. It may be easier to prove that $\mathbb{Q}(\sqrt{p^{2r}+1})$ satisfies this new condition for infinitely many r. But the authors don't know how to do it.

1.3. **On p, r such that $\mathbb{Q}(\sqrt{p^{2r}+1}) = \mathbb{Q}(\sqrt{2})$.** We prove that, for a fixed p, the fields $\mathbb{Q}(\sqrt{p^{2r}+1})$ are distinct except for finitely many cases where $\mathbb{Q}(\sqrt{p^{2r}+1}) = \mathbb{Q}(\sqrt{2})$. We expect that the case $\mathbb{Q}(\sqrt{p^{2r}+1}) = \mathbb{Q}(\sqrt{2})$ should never happen and show that such exceptions are related to divisibility properties of the sequence $\{G_n\}$ defined by $(1+\sqrt{2})^n = G_n + F_n\sqrt{2}$. We prove the following result in the appendix, which may be of independent interest.

Let ν_2 be the 2-adic valuation.

Theorem 1.3. *Let $l, m \in \mathbb{N}$.*

$$G_{gcd(l,m)} = \begin{cases} gcd(G_l, G_m) & \nu_2(l) = \nu_2(m) \\ 1 & \nu_2(l) \neq \nu_2(m) \end{cases}$$

The theorem is Theorem 5.2 in Appendix. It is worth pointing out that in [McC24], McConnell constructs an infinite family of non p-rational real quadratic fields based on the sequence $d_l(D)$. The sequence $d_l(D)$ also has "strong divisibility" if indexes have the same 3-adic valuation. There may be a connection between these two sequences.

1.4. **Structure of the Paper.** In Section 2, we study the general property 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 the Greenberg's conjecture for K. In the Appendix, we study properties of the sequence G_n.

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 an arbitrary real quadratic field. This congruence appears as a key step in the numerical criterion to determine non p-rationality, and when 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 field 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. Let ε be an element in $\mathbb{Z}_p^*$. Suppose that $t = \pm\varepsilon^k$ for some integer k prime to p. Then we have*

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

Proof. Assume we know $\varepsilon^{p-1} \equiv 1 \pmod{p^2\mathbb{Z}_p}$. Then $t^{p-1} = \varepsilon^{k(p-1)} \equiv 1 \pmod{p^2\mathbb{Z}_p}$.

Assume we know $t^{p-1} \equiv 1 \pmod{p^2\mathbb{Z}_p}$. Since $\varepsilon^{p-1} \equiv 1 \pmod{p\mathbb{Z}_p}$, we may assume $\varepsilon^{p-1} \equiv 1 + pl \mod p^2\mathbb{Z}_p$ for some $l \in \mathbb{Z}_p$. Hence,

$$\varepsilon^{p(p-1)} \equiv (1+pl)^p \equiv 1 \pmod{p^2\mathbb{Z}_p}.$$

Since $\gcd(k,p) = 1$, there exists integer x and y such that $xk + yp = 1$.

$$\varepsilon^{p-1} = \varepsilon^{xk(p-1)} \cdot \varepsilon^{yp(p-1)} \equiv t^{x(p-1)} \cdot 1^y \equiv 1 \pmod{p^2\mathbb{Z}_p}.$$

□

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 is 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 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 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 motivated by the proof of [ME05].

Lemma 2.4. *Let D be a positive square-free integer and $K = \mathbb{Q}(\sqrt{D})$. Assume that the old prime p is split in K. Let $t = a + b\sqrt{D}$ be a unit in $\mathcal{O}_K$,where $a, b \in \mathbb{Z}[\frac{1}{2}]$. 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 [KM03] 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

$$F_{2n} \equiv 2na \mod a^2, F_{2n-1} \equiv 1 \pmod{a^2}$$

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 $m^2p^{2r} + 1 = b^2D$, where D is a square-free integer, $r \geq 2, m, b$ are positive integers, $p \geq 3$ is an odd prime and $\gcd(p, m) = 1$. Let $K = \mathbb{Q}(\sqrt{D})$. Then p splits in the real quadratic field K.*

Proof. 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 absolute value of a real number.

Theorem 2.6. *Let $m^2p^{2r} + 1 = b^2D$, where D is a square-free integer, $r \geq 2, m, b$ are positive integers, $p \geq 3$ is an odd prime and $\gcd(p, m) = 1$. Let $K = \mathbb{Q}(\sqrt{D})$, and let ε_D 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

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

Proof. 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 $t = mp^r - b\sqrt{D} = \pm\varepsilon_D^k$ for some integer k prime to p, then the conclusion holds by lemma 2.1.

Now assume $t = mp^r - b\sqrt{D} = \pm\varepsilon_D^{p^l k}$ for some integer k prime to p and $l \geq 1$. Let $x + y\sqrt{D} := \varepsilon_D^k$, where $x, y \in \mathbb{Z}[\frac{1}{2}]$. 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 [htt], one has $v_p(\binom{p^l}{i}) = l - v_p(i)$. 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 $|\cdot|_\infty$ both side for 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 $x \in \mathbb{Z}[1/2]$, $p \mid x$, and $x \neq 0$. Hence $|x|_\infty \geq \frac{p}{2}$. Since $r = l + 1$

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

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

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

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. Empirically speaking, this case is rare. When m is odd,*

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

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 [ME05].

Lemma 2.8. *Let $p^{2r} + 1 = b^2 D$, 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 except for the finite choice of p and r such that $D = 2$.*

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 $k = 1$ except for finite choice of p and r.

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, since k is odd, let q be 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

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

where

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

Note that we can factor out v since q is odd. Notice $v^2 - w^2 D = \mathrm{Nrm}(\varepsilon_D^{k/q}) = -1$ implies that $\gcd(v, w) = \gcd(v, D) = 1$. Hence $\gcd(v, u) = 1$. Now, $p^r = uv$, 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

$$1 + \sqrt{2} = v + w\sqrt{D} = \varepsilon_D^{k/q}$$

Hence, $\varepsilon_D = 1 + \sqrt{2}$ and $k = q$. Now we have that

$$(1 + \sqrt{2})^q = p^r + b\sqrt{2}$$

Define $G_n, F_n \in \mathbb{Z}$ as $(1 + \sqrt{2})^n = G_n + F_n\sqrt{2}$. One can check that $G_{n+2} = 2G_{n+1} + G_n$. By the following Theorem in [Pet01], there is only a finite choice of n such that G_n is a perfect power. □

Theorem 2.9 (Theorem 7 in [Pet01])**.** *Let G_n be a non-degenerated second-order linear recurrence sequence and $G_{n+2} = A_1 G_{n+1} + A_2 G_n$. Then there exist effectively computable positive constants c_1 and c_2 depending only on G_0, G_1, A_1, A_2 such that if for the integers n, x, d such that $d \geq 2$ the equation*

$$G_n = x^d$$

holds, then:

(a) *If $|x| > 1$, then $\max\{|x|, n, d\} < c_1$*
(b) *If $|x| \leq 1$, then $n < c_2$.*

Remark 2.10. *Theorem 2.9 is proved independently by [Pet82] and [SS83]. The explicit bound in Theorem 2.9 is usually very large.*

Remark 2.11. *In our case, $G_{n+2} = 2G_{n+1} + G_n$ and $G_1 = 1, G_2 = 3$. Notice that Theorem 2.9 doesn't require x to be prime. We conjecture that $G_n = p^r$ has no solution (n, p, r) with p and odd prime and $r \geq 2$. The authors are unable to prove this conjecture. However, we can prove for a fixed odd p, there is at most one solution (see Lemma 5.3 in the Appendix since it is a different thread of topics). It is worth pointing out that, in [McC24], McConnell constructed an infinite family of non p-rational real quadratic fields by using a kind of strong divisibility property of the sequence $d_l(D)$ (see the Appendix 5 for the definition $d_l(D)$). In the Appendix, we prove that $\{G_n\}_n$ is also a strong divisibility sequence when indexes have the same 2-adic valuation.*

Lemma 2.12. *For $i = 1, 2$, let $p^{2r_i} + 1 = b_i^2 D_{r_i}$, where D_{r_i} is a square-free integer, $r_i \geq 2, b_i$ are positive integers, and $p \geq 3$ is an odd prime. Except for finitely many choices of p_i and r_i, we have $\mathbb{Q}(\sqrt{D_{r_1}}) = \mathbb{Q}(\sqrt{D_{r_2}})$ if and only if $r_1 = r_2$.*

Proof. By lemma 2.8, except for finite number of cases, 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 2.12, 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 $\mathbb{Q}(\sqrt{m^2p^{2r}+1})$ in the following sections.

3. p-RATIONALITY

We first recall the definition of a p-rational of a number field. It was introduced by Movahhedi and Nguyen Quang Do [Mov90] [NM90][Ngu86]. The concept has been developed and related to many arithmetic subjects (see [GC03]). For our purpose in the paper, we only care about the p-rationality of real quadratic fields. Here, we only recall the definition of p-rationality for totally real fields (see also Section 3.3.2 of [McC24] for some equivalent definitions for p-rationality of real quadratic fields).

Let K be a totally real field and p be an odd prime. Let L be the maximal abelian pro-p extension of K unramified outside p. Suppose K has r_1 real embedding and $2r_2$ complex embedding. Assume Leopoldt's conjecture holds for K. Then there are only r_2+1 independent $\mathbb{Z}_p$ extensions of K. Hence

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

where $\mathcal{T}_K$ is a finite abelian p-group. We say K is p-rational if and only if $\mathcal{T}_K = 0$. The size of $\mathcal{T}_K$ is related to the special value of L-function. The following theorem is due to Coates (see the Appendix of [Coa77]).

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 the Theorem 3.1 of Coates. Since K is a real quadratic field, $w_1(K(\mu_p)) = p$. 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 Lemma 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,

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

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 is a non p-rational real quadratic field.

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

This set contains the following subset,

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

By Lemmas 2.8 and 2.12, 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 [Gra23] and [Gra19]. In Section 4.3 of [Gra19], Gras considers the real quadratic fields $\mathbb{Q}(\sqrt{m^2p^{2r}+1})$, but he assumes that $(m^2p^{2r}+1)$ is square-free. In section 6 of [Gra23], it seems that Gras fixed $r = 2$ and let m increase to construct an infinite many non p-rational fields.

4. Iwasawa Invariants

In this section, we will consider the Iwasawa invariants μ and λ of $\mathbb{Q}(\sqrt{p^{2r}+1})$ for cyclotomic $\mathbb{Z}_p$-extension. In [Gre76], 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 [Fuk86][FK86a][FT95][Tay96][McC01]). 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 [OT97][FK05][NH88][Kra96]). In this section, we first recall a numerical criterion developed by Fukuda and Komatsu [FK86b]. 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 the generator of the principal ideal $\bar{\mathfrak{p}}^{h_K}$. Let ε_K be the fundamental unit of K. Define the integer n_1 and n_2 such that

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

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

Despite the ambiguity of α, the value of n_1 is uniquely defined 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 [Fuk86][FK86a][FT95]. Here we only recall one criterion from [FK86b].

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 prime p.

Theorem 4.1 (Fukuda and Komatsu [FK86b])**.** *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 $p^{2r} + 1 = b^2 D$, 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 $p^{2r} = b^2 D - 1 = (b\sqrt{D} + 1)(b\sqrt{D} - 1)$ 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 value of n_2 if $D \neq 2$.

Lemma 4.2. *$n_2 = r$ except for a finite choice of p and r.*

Proof. By Lemma 2.8, except for a finite choice of p and r such that $D = 2$, 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 Wieferich prime if $p^2 \mid (2^{p-1} - 1)$. It is rare that the prime p happens to be a Wieferich prime. Although the only known Wieferich primes are 1093 and 3511 [Wik24], it is conjectured that there is an infinite number of Wieferich primes. We note that Silverman [Sil88] has shown the infinitude of non Wieferich primes under the assumption of the *abc*-conjecture.

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 $\bar{\mathfrak{p}}$ 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 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 $\mu = \lambda = 0$ 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.*

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

We expect that the above family is an infinite family by computation data. However, we don't know how to prove it. As mentioned before, there are also other kinds of numerical criteria [Fuk86][FK86a][FT95] in terms of n_1 and n_2 defined above. Note that we assume p does not divide the class number of K so that $A_0 = D_0$, and hence we may apply Theorem 4.1. We may weaken this condition by just assuming $A_0 = D_0$ or applying other numerical criteria. However, the authors still do not know if there are infinitely many fields amongst $\mathbb{Q}(\sqrt{p^{2r}+1})$ for varying r that satisfy this different condition. We believe the following:

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

5. Appendix

Define $G_n, F_n \in \mathbb{Z}$ such that

$$(1+\sqrt{2})^n = G_n + F_n\sqrt{2}, \qquad n \in \mathbb{Z}.$$

Comparing $(1+\sqrt{2})^{-n} = (\sqrt{2}-1)^n$ and $(1+\sqrt{2})^n$, we have

$$G_{-n} = (-1)^n G_n, F_{-n} = F_n.$$

Lemma 5.1. *For $l, m \in \mathbb{Z}$, we have the identity*

$$G_{l+m} = 2G_mG_l - (-1)^m G_{l-m}. \tag{3}$$

Proof. Looking at $(1+\sqrt{2})^{l+m} = (1+\sqrt{2})^l(1+\sqrt{2})^m$, we have

$$G_{l+m} + F_{l+m}\sqrt{2} = (G_l + F_l\sqrt{2})(G_m + F_m\sqrt{2})$$

Thus,

$$G_{l+m} = G_l F_m + 2F_l F_m \tag{4}$$

On the other hand, since $(1+\sqrt{2})^{l-m} = (1+\sqrt{2})^l(1+\sqrt{2})^{-m}$, we have

$$G_{l-m} + F_{l-m}\sqrt{2} = \frac{G_l + F_l\sqrt{2}}{G_m + F_m\sqrt{2}} = \frac{(G_l + F_l\sqrt{2})(G_m - F_m\sqrt{2})}{(-1)^m}.$$

Thus,

$$G_{l-m} = (G_l G_m - 2F_l F_m)\cdot(-1)^m. \tag{5}$$

Combining the equation (4) and (5), we get equation (3). □

Theorem 5.2. *Let $l, m \in \mathbb{N}$. If $l, m \in \mathbb{N}$ have the same 2-adic valuation, then*

$$G_{gcd(l,m)} = gcd(G_l, G_m)$$

If the power of 2 dividing l is different from that dividing m. Then

$$gcd(G_l, G_m) = 1$$

Proof. By equation (3), we have

$$G_l = G_{l-r+r} = 2G_{l-r}G_r - (-1)^r G_{l-2r}$$

Hence

$$gcd(G_l, G_r) = gcd(G_{l-2r}, G_r)$$

For a pair $(l, r) \in \mathbb{N}^2$, we will define an operation on the pair to create a new pair (l_1, r_1) in the following way: Assume that $l \geq r$, and define the new pair by

$$l_1 = \max\{|l-2r|, |r|\}$$

$$r_1 = \min\{|l-2r|, |r|\}$$

The operation on the pair (l, r) has the following property,

$$gcd(G_l, G_r) = gcd(G_{l_1}, G_{r_1})$$

$$gcd(l, r) = gcd(l_1, r_1)$$

and

$$\max\{l, r\} \geq \max\{l_1, r_1\}$$

Notice that l, r have the same 2-valuation if and only if l_1, r_1 have the same 2-valuation. By repeating the operation on the pairs,

$$(l, r), (l_1, r_1), \cdots, (l_{n-1}, r_{n-1}), (l_n, r_n)$$

we get a sequence of pairs until

$$\max\{l_{n-1}, r_{n-1}\} = \max\{l_n, r_n\} \tag{6}$$

Assume that $l_n = r_{n-1}$, and $r_n = |l_{n-1} - 2r_{n-1}|$. By formula (6), we have $l_{n-1} = l_n = r_{n-1}$. We have $gcd(l, r) = gcd(l_{n-1}, r_{n-1}) = l_{n-1} = r_{n-1}$. Thus $gcd(G_l, G_r) = gcd(G_{l_{n-1}}, G_{r_{n-1}}) = G_{gcd(l,r)}$. Notice that $l_{n-1} = r_{n-1}$ implies that l_{n-1}, r_{n-1} have the same 2-valuation. The case happens when l, r have the same 2-valuation.

Assume that $l_n = |l_{n-1} - 2r_{n-1}|, r_n = r_{n-1}$. By formula (6), we have $l_{n-1} = |l_{n-1} - 2r_{n-1}|$. If $l_{n-1} = -l_{n-1} + 2r_{n-1}$, then $l_{n-1} = r_{n-1}$. It is the same as the previous case. If $l_{n-1} = l_{n-1} - 2r_{n-1}$, then $r_n = r_{n-1} = 0$. We have $gcd(G_l, G_r) = gcd(G_{l_n}, G_{r_n}) = 1$ since $G_0 = 1$. Notice that $l_{n-1} = 2r_{n-1}$ implies that l_{n-1}, r_{n-1} have different 2-valuation. The case happens only when l, r have different 2-valuation. □

The theorem shows that the sequence G_n is similar to a strong divisibility sequence (it is a strong divisibility sequence when indexes have the same 2-adic valuation). In [McC24], McConnell constructs an infinite family of non p-rational real quadratic fields based on the sequence $d_l(D)$ which was defined by McConnell as follows: If ε_D is the fundamental unit of K, let

$$u = \begin{cases} \varepsilon_D^2 & \text{if } \mathrm{Nrm}(\varepsilon_D) = -1 \\ \varepsilon_D & \text{else} \end{cases}$$

Then $d_l(D) = u^l + u^{-l} + 1$. The sequence $d_l(D)$ is similarly a strong divisibility sequence when indexes have the same 3-adic valuation. (see Section 3.2 of [McC24]).

Though we expect that there is no odd prime p such that $G_n = p^r$ for $r \geq 2$, the following lemma is as far as the authors can get.

Lemma 5.3. *Fix an odd prime p. Then there is at most one solution $G_n = p^r$ for some $r \geq 2$.*

Proof. By the argument of the proof for Lemma 2.8, if it has a solution then $n = q$ has to be an odd prime. Assume that there are two solutions $G_{q_1} = p^{r_1}$ and $G_{q_2} = p^{r_2}$ and q_1, q_2 are prime number. Then by the Theorem 5.2,

$$1 = G_1 = G_{gcd(q_1,q_2)} = gcd(p^{r_1}, p^{r_2}) = p^{\min\{r_1,r_2\}} \neq 1$$

Contradiction! □

References

[Ben21] Y. Benmerieme. "Les corps multi-quadratiques p-rationnels". PhD thesis. Université de Limoges, 2021.

[Bye01] D. Byeon. "Indivisibility of Class Numbers and Iwasawa *lambda*-Invariants of Real Quadratic Fields". In: *Compositio Mathematica* 126.3 (2001), pp. 249–256.

[Coa77] 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.

[FK05] 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.

[FK86a] T. Fukuda and K. Komatsu. "On $\mathbb{Z}_p$-extensions of real quadratic fields". In: *J. Math. Soc. Japan* 38.1 (1986).

[FK86b] T. Fukuda and K. Komatsu. "On $\mathbf{Z}_p$-extensions of real quadratic fields". In: *J. Math. Soc. Japan* 38.1 (1986), pp. 95–102.

[FT95] 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.

[Fuk86] T. Fukuda. "On the λ invariants of $\mathbb{Z}_p$-Extensions of Real Quadratic Fields". In: *Journal of Number Theory* 23 (1986), pp. 238–242.

[FW79] B. Ferrero and L. Washington. "The Iwasawa Invariant μ_p Vanishes for Abelian Number Fields". In: *Annals of Mathematics* (1979), pp. 377–395.

[GC03] G. Gras and H. Cohen. *Class Field Theory: from theory to practice*. Springer, 2003.

[Gra19] 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.

[Gra23] G. Gras. "Unlimited lists of quadratic integers of given norm application to some arithmetic properties". In: *Communications in Advanced Mathematical Sciences* (Sept. 2023).

[Gre76] R. Greenberg. "On the Iwasawa invariants of totally real number fields". In: *Amer. J. Math.* 98.1 (1976), pp. 263–284.

[htt] 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`.

[Ito12] Itoh. "On certain infinite families of imaginary quadratic fields whose Iwasawa λ-invariant is equal to 1". In: *Acta Arithmetica* 168.4 (2012).

[Iwa73] K. Iwasawa. "On $\mathbb{Z}_l$-Extensions of Algebraic Number Fields". In: *Annals of Mathematics* 98.2 (1973), pp. 246–326.

[KM03] D. Kalman and R. Mena. "The Fibonacci Numbers: Exposed". In: *Mathematics Magazine* 76.3 (2003), pp. 167–181.

[Kra96] J. Kraft. "CLASS NUMBERS AND IWASAWA INVARIANTS OF QUADRATIC FIELDS". In: *PROCEEDINGS OF THE AMERICAN MATHEMATICAL SOCIETY* 124.1 (1996), pp. 31–34.

[McC01] W. G. McCallum. "Greenberg's conjecture and units in multiple $\mathbb{Z}_p$-extensions". In: *Amer. J. Math.* 123.5 (2001), pp. 909–930.

[McC24] G. McConnell. *Some new infinite families of non-p-rational real quadratic fields*. 2024. arXiv: `2406.14632 [math.NT]`.

[ME05] M. R. Murty and J. Esmonde. *Problems in Algebraic Number Theory*. 2nd. Springer, 2005.

[Mov90] A. Movahhedi. "Sur les p-extensions des corps p-rationnels". In: *Math. Nachr.* 149 (1990), pp. 163–176.

[Ngu86] 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.

[NH88] J. Nakagawa and K. Horie. "Elliptic curves with no rational points". In: *Proc. Amer. Math. Soc.* 104.1 (1988), pp. 20–24.

[NM90] T. Nguyen Quang Do and A. Movahhedi. "Sur l'arithmétique des corps de nombres p-rationnels". In: *Séminaire de Théorie des Nombres, Paris 1987–88* (1990), pp. 155–200.

[Ono99] K. Ono. "Indivisibility of Class Numbers of Real Quadratic Fields". In: *Compositio Mathematica* 119.1 (1999), pp. 1–11.

[OT97] M. Ozaki and H. Taya. "On the Iwasawa $\lambda 2$-invariants of certain families of real quadratic fields". In: *manuscripta mathematica* 94 (1997), pp. 437–444.

[Pet01] A. Pethő. "Diophantine properties of linear recursive sequences II". In: *Acta Mathematica Academiae Paedagogicae Nyiregyhaziensis* 17 (Jan. 2001), pp. 81–96.

[Pet82] A. Pethő. "Perfect powers in second order linear recurrences". In: *J. Number Theory* 15.1 (1982), pp. 5–13.

[Sil88] J. H. Silverman. "Wieferich's criterion and the *abc*-conjecture". In: *J. Number Theory* 30.2 (1988), pp. 226–237.

[SS83] T. N. Shorey and C. L. Stewart. "On the Diophantine equation $ax^{2t} + bx^t y + cy^2 = d$ and pure powers in recurrence sequences". In: *Math. Scand.* 52.1 (1983), pp. 24–36.

[Tay96] H. Taya. "On cyclotomic $\mathbf{Z}_p$-extensions of real quadratic fields". In: *Acta Arith.* 74.2 (1996), pp. 107–119.

[Was97] L. C. Washington. *Introduction to cyclotomic fields*. Second. Vol. 83. Graduate Texts in Mathematics. Springer-Verlag, New York, 1997, pp. xiv+487.

[Wik24] Wikipedia contributors. *Wieferich prime — Wikipedia, The Free Encyclopedia*. [Online; accessed 7-July-2024]. 2024.

Email address: qipeikai@msu.edu

Michigan State University, East Lansing, Michigan, USA

Email address: mathewsonstokes@gmail.com

Randolph College, Lynchburg, Virginia, USA