

FIBONACCI SEQUENCES AND REAL QUADRATIC p -RATIONAL FIELDS

ZAKARIAE BOUAZZAOUI⁽¹⁾

ABSTRACT. We study the p -rationality of real quadratic fields in terms of generalized Fibonacci numbers and their periods modulo positive integers.

1. INTRODUCTION

Let K be a number field and p an odd prime number. The field K is said to be p -rational if the Galois group of the maximal pro- p -extension of K which is unramified outside p is a free pro- p -group of rank $r_2 + 1$, where r_2 is the number of pairs of complex embedding of K . The notion of p -rational number fields has been introduced by Movahhedi and Nguyen Quang Do [M-N], [Mo88], [Mo90], and is used for the construction of non-abelian extensions satisfying Leopoldt's conjecture. Recently, R. Greenberg used complex abelian p -rational number fields for the construction of p -adic Galois representations with open images. In these paper we study the p -rationality of real quadratic number fields. In fact, we give a generalization of a result of Greenberg [G, Corollary 4.1.5] which relates the p -rationality of the field $\mathbf{Q}(\sqrt{5})$ to properties of the classical Fibonacci numbers. More precisely, let $d > 0$ be a fundamental discriminant. Denote by ε_d and h_d the fundamental unit and the class number of the field $\mathbf{Q}(\sqrt{d})$ and let $N(\cdot)$ be the absolute norm. We associate to the field $\mathbf{Q}(\sqrt{d})$ a Fibonacci sequence $F^{(\varepsilon_d + \bar{\varepsilon}_d, N(\varepsilon_d))} = (F_n)_{n \geq 0}$ defined by $F_0 = 0$, $F_1 = 1$ and the recursion formula

$$F_{n+2} = (\varepsilon_d + \bar{\varepsilon}_d)F_{n+1} - N(\varepsilon_d)F_n, \text{ for } n \geq 0.$$

The main result of this paper is the following theorem, which describes the p -rationality in terms of Fibonacci-Wieferich prime (see Definition 3.3 for Fibonacci-Wieferich primes).

Theorem 1.1. *Let $p \geq 3$ be an odd prime number such that $p \nmid (\varepsilon_d - \bar{\varepsilon}_d)^2 h_d$. The following assertions are equivalent:*

- (1) *the field $\mathbf{Q}(\sqrt{d})$ is p -rational,*
- (2) *p is not a Fibonacci-Wieferich prime for $\mathbf{Q}(\sqrt{d})$.*

It is known that for every positive integer m , the reduction modulo m of the sequence $(F_n)_n$ is periodic of period a positive integer $k(m)$ [Wall, Theorem 1.], [D-R]. Using this fact and properties of these periods, we give another characterization of the p -rationality of $\mathbf{Q}(\sqrt{d})$ in terms of the periods of the associated Fibonacci numbers.

Proposition 1.2. *Let $p \geq 3$ be a prime number such that $p \nmid (\varepsilon_d - \bar{\varepsilon}_d)^2 h_d$. Then the following assertions are equivalent:*

- (1) *the field $\mathbf{Q}(\sqrt{d})$ is p -rational,*
- (2) *$k(p) \neq k(p^2)$.*

For the classical Fibonacci sequence, namely $a = b = 1$, D.D. Wall is the first to study these periods in [Wall], where he proved many properties of these integers. One problem encountered by Wall in his paper is the study of the hypothesis $k(p) \neq k(p^2)$. He asked whether

2010 *Mathematics Subject Classification.* 11B39, 11M06, 20G05.

Key words and phrases. p -rational fields, Fibonacci numbers, periods, L -functions.

the equality $k(p) = k(p^2)$ is possible. This question is still open with strong numerical evidence [E-J]. By Proposition 1.2, it is equivalent to whether the number field $\mathbf{Q}(\sqrt{5})$ is not p -rational for some prime number p . It is generalized to Fibonacci sequences $F^{(a,b)}$ where for some sequences we have an affirmative answer, for example the Fibonacci sequence $F^{(2,-1)}$ gives that $k(13) = k(13^2)$ and $k(31) = k(31^2)$, which means that the field $\mathbf{Q}(\sqrt{2})$ is not p -rational for $p = 13, 31$. Under the light of the above characterization of the p -rationality, the conjecture of G. Gras [Gr, Conjecture 7.9] on the p -rationality of real quadratic fields, it is suggested that for almost all primes p we have $k(p) \neq k(p^2)$.

2. p -RATIONAL FIELDS

In this section we give a characterization of the p -rationality of real quadratic fields in terms of values of the associated L -functions at odd negative integers. In fact, the p -rationality of totally real abelian number fields K is intimately related to special values of the associated zeta functions ζ_K . The relation is as follows. For any finite set Σ of primes of K , we denote by $G_\Sigma(K)$ the Galois group of the maximal pro- p -extension of K which is unramified outside Σ . Let S be the finite set of primes $S_p \cup S_\infty$, where S_∞ is the set of infinite primes of K and S_p is the primes above p in K . It is known that the group $G_{S_p}(K)$ is a free pro- p -group on $r_2 + 1$ generators if and only if the second Galois cohomology group $H^2(G_{S_p}(K), \mathbf{Z}/p\mathbf{Z})$ vanishes. This vanishing is related to special values of the zeta function ζ_K via the conjecture of Lichtenbaum. More precisely, let \mathcal{G}_S be the Galois group of the maximal extension of K which is unramified outside S . The main conjecture of Iwasawa theory (now a theorem of Wiles [W90]) relates the order of the group $H^2(\mathcal{G}_S, \mathbf{Z}_p(i))$, for even integers i , to the p -adic valuation of $\zeta_K(1-i)$ by the p -adic equivalence:

$$w_i(K)\zeta_K(1-i) \sim_p |H^2(\mathcal{G}_S, \mathbf{Z}_p(i))|, \quad (1)$$

where for any integer i , $w_i(F)$ is the order of the group $H^0(G_F, \mathbf{Q}_p/\mathbf{Z}_p(i))$, and \sim_p means having the same p -adic valuation, see e.g. [Kol]. Moreover, the group $H^2(\mathcal{G}_S, \mathbf{Z}_p(i))$ vanishes if and only if $H^2(\mathcal{G}_S, \mathbf{Z}/p\mathbf{Z}(i))$ vanishes. Let μ_p be the group of p -th unity. The periodicity of the groups $H^2(\mathcal{G}_S, \mathbf{Z}/p\mathbf{Z}(i))$ modulo $\delta = [K(\mu_p) : K]$ gives that

$$H^2(\mathcal{G}_S, \mathbf{Z}/p\mathbf{Z}(i)) \cong H^2(\mathcal{G}_S, \mathbf{Z}/p\mathbf{Z}(i + j\delta)),$$

for any integer j . In addition, since p is odd, the vanishing of the group $H^2(\mathcal{G}_S, \mathbf{Z}/p\mathbf{Z}(i))$ is equivalent to the vanishing of the group $H^2(G_{S_p}(K), \mathbf{Z}/p\mathbf{Z}(i))$. Number fields such that $H^2(G_{S_p}(K), \mathbf{Z}/p\mathbf{Z}(i)) = 0$ are called (p, i) -regular [A]. In particular, the field K is p -rational if and only if $w_{p-1}(K)\zeta_K(2-p) \sim_p 1$. This leads to the following characterization of the p -rationality of totally real number fields.

Proposition 2.1. *Let p be an odd prime number which is unramified in an abelian totally real number field K . Then we have the equivalence*

$$K \text{ is } p\text{-rational} \Leftrightarrow L(2-p, \chi) \text{ is a } p\text{-adic unit}, \quad (2)$$

where χ is ranging over the set of irreducible characters of $\text{Gal}(K/\mathbf{Q})$.

Proof. First, the zeta function ζ_K decomposes in the following way:

$$\zeta_K(2-p) = \zeta_{\mathbf{Q}}(2-p) \times \prod_{\chi \neq 1} L(2-p, \chi).$$

Second, it is known that $\zeta_{\mathbf{Q}}(2-p)$ is of p -adic valuation -1 and that $w_{p-1}(K)$ has p -adic valuation 1, giving that $w_{p-1}(K)\zeta_K(2-p) \sim_p 1$. Then from (1) we obtain the formula

$$\prod_{\chi \neq 1} L(2-p, \chi) \sim_p |H^2(\mathcal{G}_S, \mathbf{Z}_p(p-1))|.$$

Since, for every character $\chi \neq 1$, the value $L(2 - p, \chi)$ is a p -integer [Wa, Corollary 5.13], we have $H^2(\mathcal{G}_S, \mathbf{Z}_p(p - 1)) = 0$ if and only if for every $\chi \neq 1$, $L(2 - p, \chi)$ is a p -adic unit. Furthermore, the vanishing of the group $H^2(\mathcal{G}_S, \mathbf{Z}_p(p - 1))$ is equivalent to the vanishing of the group $H^2(\mathcal{G}_S, \mathbf{Z}/p\mathbf{Z}(p - 1))$, which turns out to be equivalent to the vanishing of $H^2(G_{S_p}(K), \mathbf{Z}/p\mathbf{Z})$ (by the above mentioned periodicity statement). This last vanishing occurs exactly when the field K is p -rational. ■

In the particular case of a real quadratic field $K = \mathbf{Q}(\sqrt{d})$, we have the decomposition

$$\zeta_K(2 - p) = \zeta_{\mathbf{Q}}(2 - p)L(2 - p, \left(\frac{d}{\cdot}\right)),$$

where $\left(\frac{d}{\cdot}\right)$ is the quadratic character associated to the field $K = \mathbf{Q}(\sqrt{d})$.

Corollary 2.2. *For every odd prime number $p \nmid d$, we have the equivalence*

$$\mathbf{Q}(\sqrt{d}) \text{ is } p\text{-rational} \Leftrightarrow L(2 - p, \left(\frac{d}{\cdot}\right)) \not\equiv 0 \pmod{p}. \quad (3)$$

■

Remark 2.3. *The properties of special values of p -adic L -functions tells us that the p -rationality is related to the class number and the p -adic regulator. More precisely, let K be a totally real number field of degree g . Under the Leopoldt conjecture, class field theory gives that $G_{S_p}(K)^{ab} \cong \mathbf{Z}_p^{r_2+1} \times \mathcal{T}_K$, where \mathcal{T}_K is the \mathbf{Z}_p -torsion of $G_{S_p}(K)^{ab}$. Then the field K is p -rational precisely when $\mathcal{T}_K = 0$ [M-N, Théorème et Definition 1.2]. Moreover, the order of \mathcal{T}_K satisfies*

$$|\mathcal{T}_K| \sim_p w(K(\mu_p)) \prod_{v|p} (1 - N(v)^{-1}) \cdot \frac{R_p(K) \cdot h_K}{\sqrt{|d_K|}}, \quad (4)$$

([Coa, app]), where h_K is the class number, $R_p(K)$ is the p -adic regulator, $N(v)$ is the absolute norm of v , $w(K(\mu_p)) = |\mu(K(\mu_p))|$ the number of roots of unity of $K(\mu_p)$ and d_K is the discriminant of the number field K . Hence for every odd prime number p such that $(p, d_K h_K) = 1$, the field K fails to be p -rational if and only if $v_p(R_p(K)) > g - 1$.

Under the light of Remark 2.3, for a real quadratic field $\mathbf{Q}(\sqrt{d})$ we have the equivalence

$$\mathbf{Q}(\sqrt{d}) \text{ is } p\text{-rational} \Leftrightarrow R_p(\mathbf{Q}(\sqrt{d})) \not\equiv 0 \pmod{p^2}. \quad (5)$$

Recall that $R_p(\mathbf{Q}(\sqrt{d})) = \log_p(\varepsilon_d)$, where ε_d is a fundamental unit of K and \log_p is the p -adic logarithm.

3. FIBONACCI NUMBER

The classical Fibonacci sequence is an interesting linear recurrence sequence, in part because of its applications in several areas of sciences. Here we consider a class of linear recurrence sequences which arise from real quadratic fields and that we use for the study of the p -rationality of these fields. As mentioned in the introduction, Greenberg [G, Corollary 4.1.5.] used classical Fibonacci numbers to give a characterization for the p -rationality of the field $\mathbf{Q}(\sqrt{5})$. In this paper we give a generalization of this result to any real quadratic field. The Fibonacci numbers associated to real quadratic fields are given as follows. Let $d > 0$ be a fundamental discriminant and let h_d, ε_d be respectively the class number and the fundamental unit of the field $\mathbf{Q}(\sqrt{d})$ with ring of integers \mathcal{O}_d . We denote by $\bar{\varepsilon}_d$ the conjugate of ε_d and $N(\cdot)$ the absolute norm. Define the sequence $F^{(\varepsilon_d + \bar{\varepsilon}_d, N(\varepsilon_d))} = (F_n)_n$ such that $F_0 = 0$, $F_1 = 1$ and

$$F_{n+2} = (\varepsilon_d + \bar{\varepsilon}_d)F_{n+1} - N(\varepsilon_d)F_n.$$

The Binet formula [D-R, page 173] gives that

$$F_n = \frac{\varepsilon_d^n - \bar{\varepsilon}_d^n}{\varepsilon_d - \bar{\varepsilon}_d}, \quad \forall n \geq 0.$$

We establish a relation between Fibonacci numbers and the p -adic regulator which allows us to prove the main result.

Definition 3.1. *Let a be a non trivial element of the ring of integers of the field $\mathbf{Q}(\sqrt{d})$ such that $(a, p) = 1$. Then the prime p is said to be Wieferich of basis a if the following congruence holds:*

$$a^{p^r-1} - 1 \equiv 0 \pmod{p^2},$$

where r is the residue degree of p in the quadratic field $\mathbf{Q}(\sqrt{d})$. Otherwise, the prime number p is said to be non-Wieferich of basis a .

We have the following equality

$$\log_p((\varepsilon_d^{p^r-1} - 1) + 1) = (\varepsilon_d^{p^r-1} - 1) - \frac{1}{2}(\varepsilon_d^{p^r-1} - 1)^2 + \dots$$

where \log_p is the p -adic logarithm and as before r is the residue degree of p in the quadratic field $\mathbf{Q}(\sqrt{d})$. Since $R_p = \log_p(\varepsilon_d)$ and the group $(\mathcal{O}_d/p\mathcal{O}_d)^\times$ is cyclic of order $p^r - 1$, where \mathcal{O}_d is the ring of integers of $\mathbf{Q}(\sqrt{d})$, we obtain the equivalences

$$\begin{aligned} \varepsilon_d^{p^r-1} - 1 \not\equiv 0 \pmod{p^2} &\Leftrightarrow R_p \equiv p \pmod{p^2}, \\ &\Leftrightarrow R_p \not\equiv 0 \pmod{p^2}. \end{aligned} \tag{6}$$

Then combining this last equivalence with the equivalence (5) we obtain

Proposition 3.2. *Let p be an odd prime number such that $p \nmid dh_d$. Then the field $\mathbf{Q}(\sqrt{d})$ is p -rational if and only if p is a non-Wieferich prime of basis ε_d .*

■

Very little is known about these primes and it is conjectured that the set of Wieferich primes is of density zero [Si]. In the following we are interested with the set of Fibonacci-Wieferich primes defined as follows.

Definition 3.3. *A prime number p is said to be a Fibonacci-Wieferich prime for the field $\mathbf{Q}(\sqrt{d})$ if*

$$F_{p-(\frac{d}{p})} \equiv 0 \pmod{p^2},$$

where $(\frac{d}{p})$ is the Legendre symbol associated to the quadratic field $\mathbf{Q}(\sqrt{d})$.

We give the main result of this section which describe the p -rationality in terms of Fibonacci-Wieferich primes.

Theorem 3.4. *Let $p \geq 5$ be a prime number such that $p \nmid (\varepsilon_d - \bar{\varepsilon}_d)^2 h_d$. Then the following assertions are equivalent:*

- (1) *the field $\mathbf{Q}(\sqrt{d})$ is p -rational,*
- (2) *p is not a Fibonacci-Wieferich prime for $\mathbf{Q}(\sqrt{d})$.*

Proof. Using the equivalence (6), it suffices to prove that:

$$\varepsilon_d^{p^r-1} - 1 \not\equiv 0 \pmod{p^2} \Leftrightarrow F_{p-(\frac{d}{p})} \not\equiv 0 \pmod{p^2}. \tag{7}$$

Let $Q_p(\varepsilon_d)$ be the residue class

$$\frac{\varepsilon_d^{p^r-1} - 1}{p} \pmod{p}.$$

A prime number p satisfying $Q_p(\varepsilon_d) \not\equiv 0 \pmod{p}$ is non-Wieferich of basis ε_d . First suppose that $(\frac{d}{p}) = 1$. Then $r = 1$ and

$$Q_p(\varepsilon_d) \equiv \frac{\varepsilon_d^{p-1} - 1}{p} \pmod{p}. \quad (8)$$

The Binet formula gives that

$$(\varepsilon_d - \bar{\varepsilon}_d)F_{p-1} = \varepsilon_d^{p-1} - \bar{\varepsilon}_d^{p-1} = \varepsilon_d^{1-p}(\varepsilon_d^{(p-1)} - 1)(\varepsilon_d^{(p-1)} + 1).$$

Since ε_d is a unit and $p \nmid (\varepsilon_d - \bar{\varepsilon}_d)$, we have $\varepsilon_d^{1-p}(\varepsilon_d^{(p-1)} + 1)(\varepsilon_d - \bar{\varepsilon}_d) \not\equiv 0 \pmod{p}$. Hence we obtain the equivalence

$$Q_p(\varepsilon_d) \not\equiv 0 \pmod{p} \Leftrightarrow F_{p-1} \not\equiv 0 \pmod{p^2}. \quad (9)$$

Second, suppose that the prime number p is inert in the field $\mathbf{Q}(\sqrt{d})$. Then we have

$$Q_p(\varepsilon_d) \equiv \frac{\varepsilon_d^{p^2-1} - 1}{p} \pmod{p}. \quad (10)$$

The Galois group of $\mathbf{Q}(\sqrt{d})/\mathbf{Q}$ is generated by an element σ of order two such that $\sigma(\varepsilon_d) = \bar{\varepsilon}_d$. Since the group $(\mathcal{O}_d/p\mathcal{O}_d)^\times$ is cyclic of order p^2-1 , we have $\varepsilon_d^{p+1} \equiv x \pmod{p}$ for some $x \in \mathbf{Z}$. Hence $\bar{\varepsilon}_d^{p+1} \equiv x \pmod{p}$ and $F_{p+1} \equiv 0 \pmod{p}$. Note that since

$$F_{p+1} = (\varepsilon_d - \bar{\varepsilon}_d)^{-1} \bar{\varepsilon}_d^{p+1} (\varepsilon_d^{2(p+1)} - 1),$$

we have

$$\varepsilon_d^{2(p+1)} - 1 \equiv 0 \pmod{p}.$$

Moreover,

$$Q_p(\varepsilon_d) = \frac{1}{p}(\varepsilon_d^{p^2-1} - 1) = \frac{1}{p}((\varepsilon_d^{2(p-1)})^{\frac{p-3}{2}} - 1) = \frac{1}{p}(\varepsilon_d^{2(p+1)} - 1)(\varepsilon_d^{2(p+1)\frac{p-1}{2}} + \dots + 1).$$

Since $x^2 \equiv 1 \pmod{p}$, we then obtain the congruence

$$Q_p(\varepsilon_d) \equiv \frac{1}{p} \frac{p-1}{2} (\varepsilon_d^{2(p+1)} - 1) \pmod{p}.$$

Hence we have the equivalence

$$Q_p(\varepsilon_d) \not\equiv 0 \pmod{p} \Leftrightarrow F_{p+1} \not\equiv 0 \pmod{p^2}. \quad (11)$$

Then in all cases we obtain that the field $\mathbf{Q}(\sqrt{d})$ is p -rational precisely when p is not a Fibonacci-Wieferich prime. ■

Using this characterization of the p -rationality on pariGP, we obtain some numerical evidence for the primes p for which a given real quadratic number field is not p -rational.

Discriminant	Primes < 10^9
5	
8	13, 31, 1546463
12	103
13	241
17	
21	46179311
24	7, 523
28	
29	3, 11
33	29, 37, 6713797
37	7, 89, 257, 631
40	191, 643, 134339, 25233137
41	29, 53, 7211
44	
53	5
56	6707879, 93140353
57	59, 28927, 1726079, 7480159
60	181, 1039, 2917, 2401457
61	
65	1327, 8831, 569831
69	5, 17, 52469057
73	5, 7, 41, 3947, 6079
76	79, 1271731, 13599893, 31352389
77	3, 418270987
85	3, 204520559
88	73, 409, 43, 28477
89	5, 7, 13, 59
92	7, 733
93	13
97	17, 3331

With the help of these results and further computations, we could construct examples of multi-quadratic p -rational fields. The first example is the field $K_1 = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \sqrt{-1})$, which is p -rational for all primes $100 < p < 1000$ except for $p = 103, 173, 181, 191, 199, 227, 251, 269, 409, 523, 571, 577, 643, 859$. Another example is the field $K_2 = \mathbf{Q}(\sqrt{13}, \sqrt{17}, \sqrt{19}, \sqrt{23}, \sqrt{29}, \sqrt{-1})$. The field K_2 is p -rational for all primes $100 < p < 1000$ except for $151, 197, 227, 241, 307, 337, 401, 457, 487, 593, 643, 709, 719, 733, 809, 839$. Hence for every prime $100 < p < 1000$ such that $p \neq 227, 643$, there exist a p -rational field of degree 2^t for any $1 \leq t \leq 6$.

The above examples are weak numerical evidence to a conjecture proposed by Greenberg:

Conjecture 1. ([G, Conjecture 4.2.1.]) *For any odd prime p and for any $t \geq 1$, there exists a p -rational field K such that $\text{Gal}(K/\mathbf{Q}) \cong (\mathbf{Z}/2\mathbf{Z})^t$.*

As an important consequence of this conjecture, Greenberg proved the following proposition.

Proposition 3.5. [G, Proposition 6.2.2] *Suppose that K is a complex p -rational number field and that $\text{Gal}(K/\mathbf{Q})$ is isomorphic to $(\mathbf{Z}/2\mathbf{Z})^t$, where $t \geq 4$. Let n be an integer such that*

$4 \leq n \leq 2^{t-1} - 3$. Then there exists a continuous homomorphism

$$\rho : G_{\mathbf{Q}} \rightarrow GL_n(\mathbf{Z}_p),$$

with open image.

Based on the above computations and Proposition 3.5, we have the following corollary.

Corollary 3.6. *For any integer $4 \leq n \leq 2^5 - 3$ and any prime $100 < p < 1000$ such that $p \neq 227, 643$, there exists a p -adic Galois representation*

$$\rho : G_{\mathbf{Q}} \rightarrow GL_n(\mathbf{Z}_p),$$

with open image.

Another characterization of the p -rationality is given in terms of periods of Fibonacci sequences modulo p and p^2 . Let $F^{(a,b)}$ be a Fibonacci sequence and m a positive integer such that $(b, m) = 1$. As mentioned above the sequence $F^{(a,b)} \pmod{m}$ is periodic of period $k(m)$. Wall studied these periods for classical Fibonacci sequence and general results are obtained in [R, page 374-376]. We describe the p -rationality of real quadratic fields in terms of periods of Fibonacci sequence associated to these fields.

Theorem 3.7. [E-J, Proposition 3.2.4]

$$\text{The equality } k(p) = k(p^2) \text{ holds if and only if } F_{p-(\frac{d}{p})} \equiv 0 \pmod{p^2}. \quad (12)$$

Proposition 1.2 follows from Theorem 3.4 and Theorem 3.7. For the classical Fibonacci numbers F_n , the field $\mathbf{Q}(\sqrt{5})$ is p -rational precisely when p is not a Fibonacci-Wieferich prime [G, Corollary 4.1.5]. It is known that up to 6.7×10^{15} there is no Fibonacci-Wieferich primes [F-K]. Greenberg pointed out in [G] that such primes are quite rare, they have trivial density if we assume G. Gras Conjecture, which asserts that a number field is p -rational for almost all primes. Theorem 3.7, gives that the field $\mathbf{Q}(\sqrt{d})$ is p -rational if and only if $k(p) \neq k(p^2)$. According to the table above there is fundamental discriminants d such that there exist primes p for which $k(p) = k(p^2)$. As an example we mentioned the case of $\mathbf{Q}(\sqrt{2})$ where $k(13) = k(13^2)$. Note that up to 10^9 , for some discriminants we still have no primes satisfying the equality of Wall such as 17, 28, 44, 61.

4. WILLIAMS CONGRUENCE

Let d be a positive fundamental discriminant and p be an odd prime number such that $p \nmid d$. We are interested with the numbers $F_{p-(\frac{d}{p})}$. In the classical case, namely the field $\mathbf{Q}(\sqrt{5})$, we have explicit formula for the quotient $F_{p-(\frac{d}{p})}/p$ [Wi, Theorem 4.1]. For the general case we have a result due to H.C. Williams in [Wi] which describes these quotients for any real quadratic field. The results obtained in the above section, combined with the formula proved by Williams gives another characterization of the p -rationality of real quadratic fields. For an integer n , let $\{n\}$ be the least non-negative residue of n modulo d . The integer p' represents the inverse of p modulo d and $(\frac{d}{\cdot})$ is the Legendre symbol. Consider the following sum of characters:

$$\beta_p(i) = \sum_{j=1}^{\{p'i\}-1} \left(\frac{d}{j}\right).$$

Then the result of Williams is as follows:

Theorem 4.1. [Wi] *Let p be an odd prime number such that $p \nmid d$. Then*

$$h_d F_{p-(\frac{d}{p})}/p \equiv -2 \left(\frac{d}{p}\right) N^{\frac{(\frac{d}{p})-1}{2}} \sum_{i=1}^{\frac{p-1}{2}} \beta_p(i) \frac{1}{i} \pmod{p}, \quad (13)$$

where h_d is the class number of the field $\mathbf{Q}(\sqrt{d})$, and $\frac{1}{i}$ is the inverse of i modulo p .

An interesting problem of combinatorics and additive number theory is the study of sums of reciprocals in finite fields. Here we are concerned with the linear combinations

$$\sum_{i=1}^d \beta_p(i) \alpha_p(i) \pmod{p},$$

where

$$\alpha_p(i) = \sum_{\substack{1 \leq k \leq \frac{p-1}{2} \\ k \equiv i \pmod{d}}} \frac{1}{k}.$$

We have the following description of the p -rationality of the field $\mathbf{Q}(\sqrt{d})$.

Theorem 4.2. *If p does not divide $(\varepsilon_d - \bar{\varepsilon}_d)^2$, then*

$$\mathbf{Q}(\sqrt{d}) \text{ is } p\text{-rational} \Leftrightarrow \sum_{i=1}^d \beta_p(i) \alpha_p(i) \not\equiv 0 \pmod{p}. \quad (14)$$

Proof. It is known that $F_{p-(\frac{d}{p})} \equiv 0 \pmod{p}$ [Wi, page 431 formula (1.2)]. Then by Theorem 1.1, the field $\mathbf{Q}(\sqrt{d})$ is p -rational if and only if $h_d F_{p-(\frac{d}{p})}/p \not\equiv 0 \pmod{p}$. Using Theorem 4.1, this occurs precisely when

$$-2\left(\frac{d}{p}\right) N^{\frac{(\frac{d}{p})-1}{2}} \sum_{i=1}^{\frac{p-1}{2}} \beta_p(i) \frac{1}{i} \not\equiv 0 \pmod{p}.$$

Since p is an odd prime number and the term $2\left(\frac{d}{p}\right) N^{\frac{(\frac{d}{p})-1}{2}}$ equals 1 or 2, the field $\mathbf{Q}(\sqrt{d})$ is p -rational if and only if

$$\sum_{i=1}^{\frac{p-1}{2}} \beta_p(i) \frac{1}{i} \not\equiv 0 \pmod{p}. \quad (15)$$

Recall that for any integer i , $\{i\}$ is the least non-negative residue class of i modulo d . Hence by definition we have $\{i + kd\} = \{i\}$ for any integer $k \geq 0$ and the following equality holds for any integer $i \in \{1, \dots, d\}$:

$$\beta_p(i + kd) = \beta_p(i).$$

Then the terms $\frac{1}{i}$ and $\frac{1}{i+kd}$ of (15) have the same coefficient $\beta_p(i)$. For $i \in \{1, \dots, d\}$ regrouping the integers $\frac{1}{j}$ such that j lies in the equivalence class of i modulo d and $j \in \{1, \dots, \frac{p-1}{2}\}$, the sum in (15) can be written

$$\sum_{i=1}^{\frac{p-1}{2}} \beta_p(i) \frac{1}{i} = \sum_{i=1}^d \beta_p(i) \alpha_p(i).$$

Then the field $\mathbf{Q}(\sqrt{d})$ is p -rational if and only if $\sum_{i=1}^d \beta_p(i) \alpha_p(i) \not\equiv 0 \pmod{p}$. ■

As a consequence we have the following characterization of the p -rationality of the field $\mathbf{Q}(\sqrt{5})$.

Corollary 4.3. *For every prime $p \equiv 1 \pmod{5}$, the field $\mathbf{Q}(\sqrt{5})$ is p -rational if and only if*

$$\alpha_p(1) + \alpha_p(2) - \alpha_p(4) + 2\alpha_p(5) \not\equiv 0 \pmod{p}. \quad (16)$$

Proof. Let ℓ be a prime number, then $\left(\frac{5}{\ell}\right) = 1$ if and only if $\ell \equiv 1, 4 \pmod{5}$, and $\left(\frac{5}{\ell}\right) = -1$ if and only if $\ell \equiv 2, 3 \pmod{5}$. Since $p \equiv 1 \pmod{5}$, we have for $i \in \{1, \dots, 5\}$,

$$\beta_p(i) = \sum_{j=1}^{i-1} \left(\frac{5}{j}\right),$$

such that $\beta_p(1) = 1$, $\beta_p(2) = 1$, $\beta_p(3) = 0$, $\beta_p(4) = -1$ and $\beta_p(5) = 2$. ■

If we fix the prime number p , we obtain a description of the set of fundamental discriminants d for which the field $\mathbf{Q}(\sqrt{d})$ is p -rational. For the particular cases $p = 3$ and $p = 5$ we obtain the following proposition.

Proposition 4.4. *Let d be a fundamental discriminant such that $3, 5 \nmid (\varepsilon_d - \bar{\varepsilon}_d)^2$ then we have the equivalence:*

- (1) $\mathbf{Q}(\sqrt{d})$ is 3-rational $\Leftrightarrow \beta_3(1) \not\equiv 0 \pmod{3}$,
- (2) $\mathbf{Q}(\sqrt{d})$ is 5-rational $\Leftrightarrow \beta_5(1) \not\equiv 2\beta_5(2) \pmod{5}$.

Proof. By Theorem 4.1, we have for $p = 3$ the equality

$$\sum_{i=1}^{\frac{3-1}{2}} \beta_3(i) \frac{1}{i} = \beta_3(1),$$

and for $p = 5$,

$$\sum_{i=1}^{\frac{5-1}{2}} \beta_5(i) \frac{1}{i} = \beta_5(1) + 3\beta_5(2).$$

Then the equivalences in (1) and (2) follow from Theorem 4.2. ■

In general, given an odd prime number p , it is not known whether there exist infinitely many real quadratic fields which are p -rational. This is known for the cases of $p = 3$ which is proved by Dongho Byeon in [B, Theorem 1], and the other case is $p = 5$ (see [A-B]). Both cases are proved using divisibility properties of Fourier coefficients of half-integer weight modular forms.

Acknowledgement. I would like to thank my advisor J.Assim for his guidance and patience during the preparation of this paper. Many thanks goes to H.Cohen and B.Abombert for their help on pariGP computations during the Atelier pariGP in Besançon.

REFERENCES

- [A] **Assim, J.** Codescente en K-théorie étale et de nombres, manuscripta math. 86, 499-518 (1995).
- [A-B] **Assim, J.** and **Bouazzaoui, Z.** Half-integer weight modular forms and p -rational fields. preprint
- [B] **Byeon, D.** Indivisibility of special values of Dedekind zeta functions of real quadratic fields. acta arithmetica-warszawa, 109(3), 231-235, (2003).
- [Coa] **Coates, J.** p -adic L-functions and Iwasawa's theory. dans Algebraic number fields Proc. Sympos. Durham, Academic Press (1977).
- [D-R] **Dan, K.** and **Robert, M.** The Fibonacci numbers:exposed. Mathematics magazine 76.3, 167-181 (2003).
- [E-J] **Elsenhans, A.S.** and **Jahnel, J.** The Fibonacci sequence modulo p^2 - An investigation by computer for $p < 10^{14}$ The On-Line Encyclopedia of Integer Sequences (2004).
- [F-K] **François, G.D.** and **Klyve, D.** A Wieferich Prime Search up to 6.7×10^{15} , Journal of Integer Sequences, Vol. 14 (2011).
- [Gr] **Gras, G.** Les θ -régulateurs locaux d'un nombre algébrique. conjectures p -adiques. Canad.J.Maths, pp. 571-624 (2016).
- [G] **Greenberg, R.** Galois representations with open image. Annales mathématiques du Québec, 40(1), 83-119 (2016).
- [G-M] **Graves, H.** and **Murty, M. R.** The abc conjecture and non-Wieferich primes in arithmetic progressions. Journal of Number Theory, 133(6), 1809-1813 (2013).
- [Ha] **Hatada, K.** Mod 1 distribution of Fermat and Fibonacci quotients and values of zeta functions at $2-p$, Comment. Math. Univ. St. Pauli 36, 41-51 (1987).
- [Kol] **Kolster, M.** Kolster, M. K-theory and arithmetic (No. INIS-XA-986) (2003).
- [Mo88] **Movahhedi, A.** Sur les p -extensions des corps p -rationnels, These Paris VII (1988).
- [Mo90] **Movahhedi, A.** Sur les p -extensions des corps p -rationnels, Math. Nach, 149, 163-176 (1990).
- [M-N] **Movahhedi, A.** and **Nguyen Quang Do.** Sur l'arithmétique des corps de nombres p -rationnels, Séminaire de théorie des nombres de Paris, 1987-1988, Birkhäuser, Vol 81, 155-200 (1990).

- [P] **PARI Group**. Bordeaux. PARI/GP, version 2.10.0, (2017).
- [R] **Renault, M.** The period, rank, and order of the (a, b) -Fibonacci sequence mod m . *Mathematics Magazine* 86.5: 372-380 (2013).
- [Si] **Silverman, J. H.** Wieferich's criterion and the abc-conjecture. *Journal of Number Theory*, 30(2). 226-237 (1988).
- [Wall] **Wall, D. D.** Fibonacci series modulo m , *Amer. Math. Monthly* 67. 525-532 (1960).
- [Wa] **Washington, L.** *Introduction to Cyclotomic Fields* (2nd ed.), Graduate Texts in Math. 83, Springer-Verlag (1997).
- [W90] **Wiles, A.** The Iwasawa conjecture for totally real fields. *Annals of mathematics*, 131(3), 493-540 (1990).
- [Wi] **Williams H.C.** Some formulas concerning the fundamental unit of a real quadratic field. *Discrete mathematics*. 17;92(1-3):431-40 (1991).

⁽¹⁾ UNIVERSITÉ MOULAY ISMAÏL, DÉPARTEMENT DE MATHÉMATIQUES, FACULTÉ DES SCIENCES DE MEKNÈS, B.P. 11201 ZITOUNE, MEKNÈS, MAROC.

E-mail address: z.bouazzaoui@edu.umi.ac.ma