ON THE 2-CLASS GROUP OF $\mathbb{Q}(\sqrt{5pF_p})$ WHERE F_p IS A PRIME FIBONACCI NUMBER

MOHAMMED TAOUS

Abstract. Let F_p be a prime Fibonacci number where $p > 5$. Put $\mathbf{k} = \mathbb{Q}(\sqrt{5pF_p})$ and let $\mathbf{k}_1^{(2)}$ be its Hilbert 2-class field. Denote by $\mathbf{k}_2^{(2)}$ the Hilbert 2-class field of $\mathbf{k}_1^{(2)}$ and by $G = \mathrm{Gal}(\mathbf{k}_2^{(2)}/\mathbf{k})$ the Galois group of $\mathbf{k}_2^{(2)}/\mathbf{k}$. In this paper, we characterize the structure of the 2-class group of $\mathbf{k}$ and we study the metacyclicity of G.

1. Introduction

Let d be a square-free integer and $\mathbf{k} = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : \ a, b \in \mathbb{Q}\}$ be a quadratic number field. Then we define the ring of integers of $\mathbf{k}$ by

$$\mathcal{O}_{\mathbf{k}} = \{\alpha \in \mathbf{k} : \ P(\alpha) = 0 \text{ for some monic polynomial } P \in \mathbb{Z}[X]\}.$$

$$\text{It is known that } \mathcal{O}_{\mathbf{k}} = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{d}}{2}], & \text{if } d \equiv 1 \pmod 4; \\ \mathbb{Z}[\sqrt{d}], & \text{if not.} \end{cases}$$

Two ideals I and J of $\mathcal{O}_{\mathbf{k}}$ are said to be equivalent if $I = \lambda J$ for some $\lambda \in \mathbf{k}$, this definition of equivalent is an equivalence relation. The ideal classes of $\mathcal{O}_{\mathbf{k}}$ form a finite group called the class group of $\mathbf{k}$, and will be denoted by $\mathbf{C}l(\mathbf{k})$.

We define the p-rank and the p^2-rank of $\mathbf{C}l(\mathbf{k})$ respectively as follows:

$$r_p = \dim_{\mathbb{F}_p}(\mathbf{C}l(\mathbf{k})/\mathbf{C}l(\mathbf{k})^p) \text{ and } r_{p^2} = \dim_{\mathbb{F}_p}(\mathbf{C}l(\mathbf{k})^p/\mathbf{C}l(\mathbf{k})^{p^2})$$

where $\mathbb{F}_p$ is the finite field with p elements.

Several works are interested in determining the structure of the p-class group $\mathbf{C}l_p(\mathbf{k})$, that is the Sylow p-subgroup of $\mathbf{C}l(\mathbf{k})$. For example, for $p = 2$, $r_2 = 2$ and $r_4 = 0$ or 1, we can see the works of P. Kaplan [13], and Benjamin et all [4]. As the only perfect squares in the Fibonacci sequence are $F_0 = 0$, $F_1 = F_2 = 1$ and $F_{12} = 144$ (see, e.g., [8]), then the quadratic field $\mathbf{k} = \mathbb{Q}(\sqrt{\pm F_n})$ is well defined for $n \notin \{0, 1, 2, 12\}$. On the other hand, by genus theory, the 2-class group, $\mathbf{C}l_2(\mathbf{k})$, of $\mathbf{k} = \mathbb{Q}(\sqrt{F_n})$ is trivial if and only if $F_n = m^2 p$ where p is a prime number.

Y. Kishi [14] gave an infinite family of imaginary quadratic fields $\mathbb{Q}(\sqrt{-F_n})$ with $n \equiv 25 \pmod{50}$ such that $r_5 \geq 1$. The latter author and M. Aoki gave in [1] another infinite family of pairs of imaginary quadratic fields with $r_5 \geq 1$. Motivated by these works, we thought, in a first time, studying the 2-class group of the real quadratic fields $\mathbf{k} = \mathbb{Q}(\sqrt{F_n})$. But we noticed that we cannot do it, in general, since to calculate the rank of $\mathbf{C}l_2(\mathbf{k})$, we must first calculate the prime numbers that divide square-free part of F_n. To overcome this difficulty, we changed F_n by $5pF_p$ where F_p is a prime Fibonacci number with $p > 5$, and we decided to characterize the structure of the 2-class group of $\mathbf{k}$ and to study the metacyclicity of $G = \mathrm{Gal}(\mathbf{k}_2^{(2)}/\mathbf{k})$ where $\mathbf{k}_2^{(2)}$ is the second Hilbert 2-class field of $\mathbf{k}$.

2. Some consequences of the Binet's formula

The Fibonacci numbers F_n may be defined by the recurrence relation $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$ with $F_0 = 0$ and $F_1 = 1$. In 1843, the French mathematician Jacques Philippe Marie Binet (1786- 1856) discovered that

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]. \tag{2.1}$$

This expression of F_n is called *Binet's formula.* Using this formula, we can show the well-known identities [12]:

$$2^{2n-1}F_{2n} = \sum_{k=0}^{n-1} 5^k C_{2n}^{2k+1} \text{ and } 4^n F_{2n+1} = \sum_{k=0}^{n} 5^k C_{2n+1}^{2k+1}. \tag{2.2}$$

$$F_{2n+1} = F_{n+1}^2 + F_n^2. \tag{2.3}$$

From which we deduce that all the odd divisors of F_{2n+1} are of the form $4t+1$.

Recall also that the Lucas numbers are the sequence of integers $(L_n)_{n\in\mathbb{N}}$ defined by the linear recurrence equation $L_n = L_{n-1} + L_{n-2}$ for $n \geq 2$ with $L_1 = 1$ and $L_2 = 3$.

Theorem 2.1 (Legendre, Lagrange)**.** *Let p be an odd prime integer. Then the Fibonacci number F_p and the Lucas number L_p have the following properties:*

$$F_{p\pm1} \equiv \frac{1 \pm \left(\frac{p}{5}\right)}{2} \pmod{p}, F_p \equiv \left(\frac{p}{5}\right) \pmod{p} \textit{ and } L_p \equiv 1 \pmod{p}.$$

Those extraordinary sequences have so many other properties (see, e.g., [20, 12]). We can, for example, cite the following identities:

$$F_{2n} = F_n L_n. \tag{2.4}$$

$$L_n^2 - 5F_n^2 = 4(-1)^n. \tag{2.5}$$

$$5F_{2n} = 2L_{2n+1} - L_n^2 + 2(-1)^n. \tag{2.6}$$

Corollary 2.2. *Let p be a prime > 5, and denote by $\left(\frac{\cdot}{p}\right)$ the Legendre symbol. Then the Fibonacci number F_p has the following properties:*

1. *If $p \equiv 1 \pmod 4$, then $\left(\frac{F_p}{p}\right) = 1$ and $\left(\frac{p}{5}\right) = \left(\frac{F_p}{5}\right)$.*
2. *If $p \equiv 3 \pmod 4$, then $\left(\frac{F_p}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{F_p}{5}\right)$.*

Proposition 2.3 ([15])**.** *Let $p = a^2 + b^2$ be an odd prime, and suppose a odd. Then*

$$\left(\frac{a}{p}\right) = 1, \left(\frac{b}{p}\right) = \left(\frac{2}{p}\right) \textit{ and } \left(\frac{a+b}{p}\right) = \left(\frac{2}{a+b}\right).$$

3. Preliminary

In what follows, we adopt the following notations: if $\left(\frac{a}{p}\right) = 1$ and $p \equiv 1 \pmod 4$, then $\left(\frac{a}{p}\right)_4$ will denote the rational biquadratic symbol which is equal to 1 or -1, according as $a^{\frac{p-1}{4}} \equiv 1$ or $-1 \pmod p$, in particular $\left(\frac{2}{p}\right)_4 = (-1)^{\frac{p-1}{4}}$.

Lemma 3.1 ([17])**.** *If $p > 5$ is a prime such that $p \equiv 1 \pmod 4$, then $F_{\frac{p-\left(\frac{p}{5}\right)}{2}} \equiv 0 \pmod p$ and $\left(\frac{F_{\frac{p+\left(\frac{p}{5}\right)}{2}}}{p}\right) = \left(\frac{p}{5}\right)^{\frac{p-1}{4}}$.*

Proof. From the first equality of Theorem 2.1, we conclude that

$$F_{p-\left(\frac{p}{5}\right)} \equiv 0 \pmod p \text{ and } F_{p+\left(\frac{p}{5}\right)} \equiv 1 \pmod p. \tag{3.1}$$

According to Formula (2.4), we have

$$F_{p-\left(\frac{p}{5}\right)} \equiv F_{\frac{p-\left(\frac{p}{5}\right)}{2}} L_{\frac{p-\left(\frac{p}{5}\right)}{2}} \equiv 0 \pmod p.$$

We now show that p never divides $L_{\frac{p-\left(\frac{p}{5}\right)}{2}}$.

If $\left(\frac{p}{5}\right) = -1$, then Formula (2.5) implies that $L^2_{\frac{p+1}{2}} - 5F^2_{\frac{p+1}{2}} \equiv 4(-1)^{\frac{p+1}{2}} \pmod p$. If p divides $L_{\frac{p-\left(\frac{p}{5}\right)}{2}}$, then, since $p \equiv 1 \pmod 4$, $\left(\frac{p}{5}\right) = \left(\frac{5}{p}\right) = \left(\frac{4}{p}\right) = 1$. This is absurd.

If $\left(\frac{p}{5}\right) = 1$, then by replacing, in (2.6), $2n$ by $p-1$, we get $5F_{p-1} = 2L_p - L^2_{\frac{p-1}{2}} + 2$. According to the third equality of Theorem 2.1 and to the first equality of (3.1), we have $L^2_{\frac{p-1}{2}} \equiv 4 \pmod p$, i.e., p never divides $L_{\frac{p-\left(\frac{p}{5}\right)}{2}}$. Then $F_{\frac{p-\left(\frac{p}{5}\right)}{2}} \equiv 0 \pmod p$.

Finally, from the second equality of Theorem 2.1 and (2.3), we can see that

$$\begin{aligned} F_p &= F^2_{\frac{p+\left(\frac{5}{p}\right)}{2}} + F^2_{\frac{p-\left(\frac{5}{p}\right)}{2}} \equiv F^2_{\frac{p+\left(\frac{5}{p}\right)}{2}} \pmod p \\ &\equiv \left(\frac{5}{p}\right) \equiv \left(5^{\frac{p-1}{4}}\right)^2 \pmod p. \end{aligned}$$

As p is prime, so $F_{\frac{p+\left(\frac{5}{p}\right)}{2}} \equiv \pm\left(5^{\frac{p-1}{4}}\right) \pmod p$. This gives that $\left(\frac{F_{\frac{p+\left(\frac{p}{5}\right)}{2}}}{p}\right) = \left(\frac{p}{5}\right)^{\frac{p-1}{4}}$. □

Theorem 3.2 (Burde, [7])**.** *Let $m, n \in \mathbb{N}$ be odd such that $m = a^2 + b^2$ and $n = c^2 + d^2$, where $a, b, c, d \in \mathbb{N}$, $2 \nmid ac$, and $(a, b) = (c, d) = (m, n) = 1$. Suppose that $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) = 1$. Then*

$$\left(\frac{m}{n}\right)_4 \left(\frac{n}{m}\right)_4 = \left(\frac{ac+bd}{n}\right) = \left(\frac{ac+bd}{m}\right).$$

Proposition 3.3. *Let F_p be a Fibonacci number with prime index $p \equiv 1 \pmod 4$. Then we have*

$$\left(\frac{F_p}{p}\right)_4 \left(\frac{p}{F_p}\right)_4 = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 3; \\ \left(\frac{2}{p}\right), & \text{if not.} \end{cases}$$

Proof. Let $p = a^2 + b^2$ be an odd prime, and suppose that a is odd and put $\left(\frac{p}{3}\right) = (-1)^i$. It is easy to see that $p \equiv \left(\frac{p}{3}\right) \pmod 6$, this implies that $\frac{p+\left(\frac{p}{3}\right)}{2}$ is not divisible by 3, so $F_{\frac{p+\left(\frac{p}{3}\right)}{2}}$ is odd. Since $F_p = F^2_{\frac{p+\left(\frac{p}{3}\right)}{2}} + F^2_{\frac{p-\left(\frac{p}{3}\right)}{2}}$, then the previous theorem gives that

$$\begin{aligned}
\left(\frac{F_p}{p}\right)_4 \left(\frac{p}{F_p}\right)_4 &= \left(\frac{aF_{\frac{p+\left(\frac{p}{3}\right)}{2}} + bF_{\frac{p-\left(\frac{p}{3}\right)}{2}}}{p}\right) \\
&= \begin{cases} \left(\frac{a}{p}\right)\left(\frac{F_{\frac{p+\left(\frac{p}{3}\right)}{2}}}{p}\right), & \text{if } \left(\frac{p}{3}\right) = \left(\frac{p}{5}\right); \\ \left(\frac{b}{p}\right)\left(\frac{F_{\frac{p-\left(\frac{p}{3}\right)}{2}}}{p}\right), & \text{if } \left(\frac{p}{3}\right) = -\left(\frac{p}{5}\right). \end{cases} && \text{(see the lemma 3.1)} \\
&= \begin{cases} \left((-1)^i\right)^{\frac{p-1}{4}}, & \text{if } \left(\frac{p}{3}\right) = \left(\frac{p}{5}\right); \\ \left(\frac{2}{p}\right)\left(-(-1)^i\right)^{\frac{p-1}{4}}, & \text{if } \left(\frac{p}{3}\right) = -\left(\frac{p}{5}\right). \end{cases} && \text{(Proposition 2.3)} \\
&= \left(\frac{2}{p}\right)^i .
\end{aligned}$$

$\square$

To show the following results, it suffices to use Formula (2.2) modulo 5.

Lemma 3.4. *Let F_p be a Fibonacci number with prime index $p \equiv 1 \pmod 4$. Then*

(1) $F_p \equiv p \pmod 5$.
(2) $F_{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right)(p-1) \pmod 5$.
(3) $F_{\frac{p+1}{2}} \equiv 3\left(\frac{2}{p}\right)(p+1) \pmod 5$.
(4) *If* $\left(\frac{p}{5}\right) = 1$, *then* $\left(\frac{F_p}{5}\right)_4 = \left(\frac{p}{5}\right)_4$

Corollary 3.5. *Let F_p be a Fibonacci number with prime index $p \equiv 1 \pmod 4$. If $\left(\frac{p}{5}\right) = 1$, then $\left(\frac{F_p}{5}\right)_4 \left(\frac{5}{F_p}\right)_4 = \left(\frac{p}{3}\right)$.*

Proof. Since $5=1^2+2^2$, $F_{\frac{p+(\frac{p}{3})}{2}}$ is odd and $F_p=F^2_{\frac{p+(\frac{p}{3})}{2}}+F^2_{\frac{p-(\frac{p}{3})}{2}}$, then Theorem 3.2 implies that

$$\begin{aligned}
\left(\frac{F_p}{5}\right)_4\left(\frac{5}{F_p}\right)_4 &= \left(\frac{F_{\frac{p+(\frac{p}{3})}{2}}+2F_{\frac{p-(\frac{p}{3})}{2}}}{5}\right)\\
&= \begin{cases} \left(\frac{3(\frac{2}{p})(p+1)+2(\frac{2}{p})(p-1)}{5}\right), & \text{if } \left(\frac{p}{3}\right)=1;\\ \left(\frac{(\frac{2}{p})(p-1)+6(\frac{2}{p})(p+1)}{5}\right), & \text{if } \left(\frac{p}{3}\right)=-1.\end{cases}\\
&= \begin{cases} \left(\frac{1}{5}\right)=1, & \text{if } \left(\frac{p}{3}\right)=1;\\ \left(\frac{2}{5}\right)=-1, & \text{if } \left(\frac{p}{3}\right)=-1.\end{cases}\\
&= \left(\frac{p}{3}\right).
\end{aligned}$$

□

4. Main results

Let $\mathbf{k}$ be an algebraic number field and let $\mathbf{C}l_2(\mathbf{k})$ denote its 2-class group. Denote by $\mathbf{k}_2^{(1)}$ the Hilbert 2-class field of $\mathbf{k}$ and by $\mathbf{k}_2^{(2)}$ its second Hilbert 2-class field. Put $G=\mathrm{Gal}(\mathbf{k}_2^{(2)}/\mathbf{k})$ and denote by G' its derived group; then it is well known, by class field theory, that $G/G'\simeq\mathbf{C}l_2(\mathbf{k})$.

For any prime l, $\mathfrak{l}_k$ will denote a prime ideal of $\mathbf{k}$ lies above l. We also denote by $\left(\frac{x,y}{\mathfrak{l}_\mathbf{k}}\right)$ (resp. $\left(\frac{x}{\mathfrak{l}_\mathbf{k}}\right)$) the Hilbert symbol (resp. the quadratic residue symbol) for the prime $\mathfrak{l}_k$ applied to (x,y) (resp. x). Recall that a 2-group H is said to be of type $(2^{n_1},2^{n_1},...,2^{n_s})$ if it is isomorphic to $\mathbb{Z}/2^{n_1}\mathbb{Z}\times\mathbb{Z}/2^{n_2}\mathbb{Z}\times...\mathbb{Z}/2^{n_s}\mathbb{Z}$, where $n_i\in\mathbb{N}^*$.

If $\mathbf{k}=\mathbb{Q}(\sqrt{5pF_p})$ such that F_p is a prime Fibonacci number where $p>5$, then, by genus theory, $\mathrm{rank}(\mathbf{C}l_2(\mathbf{k}))=2$. Thus $\mathbf{C}l_2(\mathbf{k})$ is of type $(2^n,2^m)$ with $n,m\in\mathbb{N}^*$. Hence group theory implies that $\mathbf{C}l_2(\mathbf{k})$ admits three normal subgroups of index 2, denote them by H_i, $i\in\{1,2,3\}$. The following diagram illustrates the situation :

$$\begin{tikzcd}
 & H_1 \arrow[dl, "2"'] & \\
\mathbf{C}l_2(\mathbf{k}) & H_2 \arrow[l, "2"'] & 1 \arrow[ul] \arrow[l] \arrow[dl] \\
 & H_3 \arrow[ul, "2"] &
\end{tikzcd}$$

On the other hand, by class field theory, each subgroup H_i of $\mathbf{C}l_2(\mathbf{k})$ is associated to a unique unramified extension F_i within $\mathbf{k}_2^{(1)}$ such that $H_i/H_i'\simeq\mathbf{C}l_2(F_i)$. The situation is represented by the following figure:

$$\begin{tikzcd}
 & F_1 \arrow[dr] & \\
\mathbf{k} \arrow[ur, "2"] \arrow[r, "2"] \arrow[dr, "2"'] & F_2 \arrow[r] & \mathbf{k}_1^{(1)} \\
 & F_3 \arrow[ur] &
\end{tikzcd}$$

According to [18, Theorem 2], the three fields F_i are given as follows:

$$F_1 = \mathbb{Q}(\sqrt{5}, \sqrt{pF_p}),\ F_2 = \mathbb{Q}(\sqrt{p}, \sqrt{5F_p}) \text{ and } F_3 = \mathbb{Q}(\sqrt{F_p}, \sqrt{5p}).$$

Recall also that a group G is said to be *metacyclic* if it has a normal cyclic subgroup H such that the quotient group G/H is cyclic. For example, if $\mathbf{C}l_2(\mathbf{k})$ is of type $(2,2)$, then G is metacyclic. More precisely and by [19], G is isomorphic to one of the following groups:

(1) Abelian 2-group of type $(2,2)$.
(2) The dihedral group.
(3) The quaternion group.
(4) The semidihedral group.

Theorem 4.1 (Main result: case $\left(\frac{p}{5}\right) = -1$)**.** *Let F_p be a prime Fibonacci number such that $p > 5$ and $\left(\frac{p}{5}\right) = -1$. Put $\mathbf{k} = \mathbb{Q}(\sqrt{5pF_p})$ and let $\mathbf{k}_1^{(2)}$ be its Hilbert 2-class field. Denote by $\mathbf{k}_2^{(2)}$ the Hilbert 2-class field of $\mathbf{k}_1^{(2)}$ and by $G = \mathrm{Gal}(\mathbf{k}_2^{(2)}/\mathbf{k})$ the Galois group of $\mathbf{k}_2^{(2)}/\mathbf{k}$. Then*

(1) *$\mathbf{C}l_2(\mathbf{k})$ is of type $(2,2)$.*
(2) *G is abelian (is of type $(2,2)$) if and only if $p \equiv 5 \pmod{24}$ or $p \equiv 3 \pmod 4$ and $F_p \equiv 1 \pmod 8$.*
(3) *If G is nonabelian, then it is quaternion, dihedral or semi-dihedral.*

Proof. If $p \equiv 1 \pmod 4$, then Corollary 2.2 implies that $\left(\frac{p}{5}\right) = \left(\frac{F_p}{5}\right) = -1$, so we use Kaplan's results on the 2-class group of the field $\mathbb{Q}(\sqrt{p_1p_2p_3})$ where $p_i \equiv 1 \pmod 4$ ([13]) to show that $\mathbf{C}l_2(k)$ is of type $(2,2)$. In the case where $p \equiv 3 \pmod 4$, we use a result of E. Benjamin and C. Snyder (namely [4, case 7, page 163]) to deduce that $\mathbf{C}l_2(k)$ is also of type $(2,2)$. According to [5], G is abelian if and only if $p \equiv 1 \pmod 4$ and $\left(\frac{F_p}{p}\right)_4 \left(\frac{p}{F_p}\right)_4 = -1$ or $p \equiv 3 \pmod 4$ and $F_p \equiv 1 \pmod 8$. This is equivalent, by Proposition 3.3 and the Chinese remainder theorem, to $p \equiv 5 \pmod{24}$ or $p \equiv 3 \pmod 4$ and $F_p \equiv 1 \pmod 8$. $\square$

Lemma 4.2. *Let F_p be a Fibonacci number with prime index $p \equiv 1 \pmod 4$. Denote by r_i the rank of the 2-class group of the field F_i, where $i \in \{1,2,3\}$. Assume $\left(\frac{p}{5}\right) = 1$.*

(1) *If $p \equiv 2 \pmod 3$, then $r_1 = r_3 = 2$ and* $r_2 = \begin{cases} 2 & \text{if } p \equiv 5 \pmod 8 \text{ or } \left(\frac{p}{5}\right)_4 \left(\frac{5}{p}\right)_4 = -1; \\ 3, & \text{if not.} \end{cases}$

(2) *If $p \equiv 1 \pmod 3$, then $r_3 = 3$ and* $r_1 = r_2 = \begin{cases} 2 & \text{if } \left(\frac{p}{5}\right)_4 \left(\frac{5}{p}\right)_4 = -1; \\ 3, & \text{if not.} \end{cases}$

Proof. This is an immediate consequence of Proposition 3.3, Corollary 3.5 and Theorem 2 of [3]. $\square$

Lemma 4.3. *Let F_p be a Fibonacci number with prime index $p \equiv 3 \pmod 4$. Denote by r_i the rank of the 2-class group of the field F_i, where $i \in \{1,2,3\}$. If $\left(\frac{p}{5}\right) = 1$, then $r_1 = r_2 = 2$ and* $r_3 = \begin{cases} 2, & \text{if } F_p \equiv 5 \pmod 8; \\ 3, & \text{if } F_p \equiv 1 \pmod 8. \end{cases}$

Proof. As the class number of $F = \mathbb{Q}(\sqrt{p})$ is odd, then the ambiguous class number formula (see [9]) implies that $r_2 = t - e - 1$, where $t = 4$ is the number of primes of F that ramify in F_2/F and e is defined by $2^e = [E_F : E_F \cap N_{F_2/F}((\mathbf{k}^*)^\times)]$. The Hasse norm theorem (see, e.g., [11, theorem 6.2, p. 179]) implies that a unit ε of F is a norm of an element of $F(\sqrt{5F_p}) = F_2$ if and only if $\left(\frac{5F_p, \varepsilon}{\mathfrak{l}_F}\right) = 1$, for all $\mathfrak{l}_F \neq \mathfrak{2}_F$ prime ideal of F. Denote by ε_p the fundamental unit of $F = \mathbb{Q}(\sqrt{p})$, so E_F, the unit group of F, is equal to $\langle -1, \varepsilon_p \rangle$. According to [2], $2\varepsilon_p$ is a square in F, then

$$\left(\frac{5F_p, \varepsilon_p}{5_{\mathbb{Q}(\sqrt{p})}}\right) = \left(\frac{\varepsilon_p}{5_{\mathbb{Q}(\sqrt{P})}}\right) = \left(\frac{\varepsilon_p}{5}\right) = \left(\frac{2}{5}\right) = -1,$$

$$\left(\frac{5F_p, -1}{\mathfrak{l}_F}\right) = \begin{cases} \left(\frac{-1}{l}\right) = 1, & \text{if } l = 5 \text{ or } l = F_p, \\ 1, & \text{if not.} \end{cases}$$

Thus we conclude that $e = 1$ and $r_2 = 2$. To prove $r_1 = 2$ and $r_3 = \begin{cases} 2, & \text{if } F_p \equiv 5 \pmod 8, \\ 3, & \text{if } F_p \equiv 1 \pmod 8, \end{cases}$ we can apply Theorem 1 of [3]. □

Theorem 4.4 (Main result: case $\left(\frac{p}{5}\right) = 1$)**.** *Let F_p be a prime Fibonacci number such that $p > 5$ and $\left(\frac{p}{5}\right) = 1$. Put $\mathbf{k} = \mathbb{Q}(\sqrt{5pF_p})$ and let $\mathbf{k}_1^{(2)}$ be its Hilbert 2-class field. Denote by $\mathbf{k}_2^{(2)}$ the Hilbert 2-class field of $\mathbf{k}_1^{(2)}$ and by $G = \mathrm{Gal}(\mathbf{k}_2^{(2)}/\mathbf{k})$ the Galois group of $\mathbf{k}_2^{(2)}/\mathbf{k}$. Then*

1. *If $p \equiv 3 \pmod 4$, then $\mathbf{C}l_2(\mathbf{k})$ is of type $(2, 2^n)$, such that $n \geq 2$ and G is metacyclic if and only if $F_p \equiv 5 \pmod 8$.*
2. *If $p \equiv 1 \pmod 4$, then G is metacyclic if and only if $p \equiv 5 \pmod{24}$ or $[p \equiv 2 \mod 3$ and $\left(\frac{p}{5}\right)_4 \left(\frac{5}{p}\right)_4 = -1]$.*

Proof. (1) If $p \equiv 3 \pmod 4$, then the last lemma and Theorem 5.1 of [6] yield that G is metacyclic if and only if $F_p \equiv 5 \pmod 8$. To show that $\mathbf{C}l_2(\mathbf{k})$ is of type $(2, 2^n)$, it suffices to prove that r_4, the 4-rank of $\mathbf{C}l_2(\mathbf{k})$, is 1. In this case, the discriminant of $\mathbf{k}$ is $\Delta = 20pF_p$, and the only possible $C4$-decomposition of Δ is $\Delta_1\Delta_2$ with

$$\begin{cases} \Delta_1 = F_p & \text{and } \Delta_2 = 20p, & \text{if } F_p \equiv 1 \pmod 8; \\ \Delta_1 = -20 & \text{and } \Delta_2 = -pF_p, & \text{if not.} \end{cases}$$

According to [16], r_4 equals the number of independent $C4$-decompositions of Δ, so $r_4 = 1$.

(2) If $p \equiv 1 \pmod 4$, then we just apply Lemma 4.2 and Theorem 5.1 of [6]. □

5. Numerical examples with all known F_p

To date, F_p is known to be prime for p =3, 4, 5, 7, 11, 13, 17, 23, 29, 43, 47, 83, 131, 137, 359, 431, 433, 449, 509, 569, 571, 2971, 4723, 5387, 9311, 9677, 14431, 25561, 30757, 35999, 37511, 50833, 81839. In addition to these proven Fibonacci primes, there have been found probable primes for p =104911, 130021, 148091, 201107, 397379, 433781, 590041, 593689, 604711, 931517, 1049897, 1285607, 1636007, 1803059, 1968721, 2904353 (See.[21]). Using the Pari software, [10], we find that there are up to now 5 primes Fibonacci numbers such that

G is nonmetacyclic. We use the following abbreviations: M means metacyclic, NM means nonmetacyclic.

p	(mod 4)	$\left(\frac{p}{5}\right)$	$\mathbf{C}l_2(\mathbf{k})$	G	p	(mod 4)	$\left(\frac{p}{5}\right)$	$\mathbf{C}l_2(\mathbf{k})$	G
7	3	-1	(2, 2)	M	14431	3	1	(2, ?)	M
11	3	1	(2, 4)	NM	25561	1	1	(2, ?)	NM
13	1	-1	(2, 2)	M	30757	1	-1	(2, 2)	M
17	1	-1	(2, 2)	M	35999	3	1	(2, ?)	NM
23	3	-1	(2, 2)	M	37511	3	1	(2, ?)	NM
29	1	1	(2, 4)	M	50833	1	-1	(2, 2)	M
43	3	-1	(2, 2)	M	81839	3	1	(2, ?)	NM
47	3	-1	(2, 2)	M	104911	3	1	(2, ?)	M
83	3	-1	(2, 2)	M	130021	1	1	(2, ?)	NM
131	3	1	(2, 4)	NM	148091	3	1	(2, ?)	NM
137	1	-1	(2, 2)	M	201107	3	-1	(2, 2)	M
359	3	1	(2, ?)	NM	397379	3	1	(2, ?)	NM
431	3	1	(2, ?)	NM	433781	1	1	(2, ?)	M
433	1	-1	(2, 2)	M	590041	1	1	(2, ?)	NM
449	1	1	(2, ?)	M	593689	1	1	(?, ?)	NM
509	1	1	(2, ?)	M	604711	3	1	(2, ?)	M
569	1	1	(2, ?)	M	931517	1	-1	(2, 2)	(2, 2)
571	3	1	(2, ?)	M	1049897	1	-1	(2, 2)	M
2971	3	1	(2, ?)	M	1285607	3	-1	(2, 2)	M
4723	3	-1	(2, 2)	M	1636007	3	-1	(2, 2)	M
5387	3	-1	(2, 2)	M	1803059	3	1	(2, ?)	NM
9311	3	1	(2, ?)	NM	1968721	1	1	(?, ?)	NM
9677	1	-1	(2, 2)	(2, 2)	2904353	1	-1	(2, 2)	M

Figure 1. Numerical examples

References

[1] M. Aoki and Y. Kishi, *An infinite family of pairs of imaginary quadratic fields with both class numbers divisible by five*, submitted

[2] A. Azizi, *Sur la capitulation des 2-classes d'idéaux de $k = \mathbb{Q}(\sqrt{2pq}, i)$, où $p \equiv -q \equiv 1$ mod 4,* Acta. Arith. **94** (2000), 383-399.

[3] A. Azizi and A. Mouhib, *Sur le rang du 2-groupe de $\mathbb{Q}(\sqrt{m}, \sqrt{d})$ où $m = 2$ ou bien un premier $p \equiv 1$* (mod 4)*,* Trans. Amer. Math. Soc. **353** (2001), 2741-2752.

[4] E. Benjamin and C. Snyder, Real quadratic number fields with 2-class group of type (2, 2), Math. Scand. **76** (1995), 161-178.

[5] E. Benjamin, F. Lemmermeyer and C. Snyder, *Real quadratic fields with abelian 2-class field tower* , J. Number Theory. **73**
(1998), 182-194.

[6] N. Blackburn, *Generalizations of certain elementary theorems on p-groups*, Proc. London Math. Soc. (3) **11** (1961),1-22

[7] K. Burde, *Ein rationales biquadratisches Reziprozitätsgesetz*, J. Reine Angew. Math. **235** (1969), 175-184.

[8] J. H. E. Cohn, *On square Fibonacci numbers*, J. London Math. Soc. **39** (1964), 537-540.

[9] C. Chevalley, *Sur la théorie du corps de classes dans les corps finis and les corps locaux*, J. Fac. Sc. Tokyo, Sect. 1, t.**2**, (1933), 365-476.

[10] The PARI Group, *PARI/GP, Bordeaux,* Version 2.7.5, Oct 26 2015, (`http://pari.math.u-bordeaux.fr`).

[11] G. Gras, *Class field theory, from theory to practice*, Springer Verlag 2003.

[12] R. P. Grimaldi, *Fibonacci and Catalan numbers. An introduction*, John Wiley & Sons, Inc., Hoboken, NJ, 2012.
[13] P. Kaplan, *Sur le* 2*-groupe de classes d'idéaux des corps quadratiques,* J. Reine angew. Math. **283/284** (1976), 313-363.
[14] Y. Kishi, *A new family of imaginary quadratic fields whose class number is divisible by five*, J. Number Theory **128** (2008), 24502458.
[15] F. Lemmermeyer, *Reciprocity Laws*, Springer Monographs in Mathematics, Springer-Verlag. Berlin 2000.
[16] L. Rédei, *Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, Math. Naturwiss. Anz. Ungar. Akad. d. Wiss. **49** (1932), 338-363.
[17] Z. H. Sun and Z. W. Sun, *Fibonacci numbers and Fermat's last theorem*, Acta Arith. **60** (1992), 371-388.
[18] B. K. Spearman, K. S. Williams, *Unramified Quadratic Extensions of a Quadratic Field*, Rocky Mountain J. Math. **25** (1995), no. 2, 783-788.
[19] O. Taussky, *A Remark on the class field tower*, J. London Math. Soc **12** (1937), 82-85.
[20] N. N. Vorobiev, *Fibonacci numbers,* Russian Academy of Sciences, 1992 (6th edition) Nauka, Moscow.
[21] Wikipedia, *Fibonacci prime,* `https://en.wikipedia.org/wiki/Fibonacci_prime#cite_note-prptop-2`

Department of Mathematics, Faculty of Sciences and Technology, Moulay Ismaïl University, Errachidia, Morocco
E-mail address: `taousm@hotmail.com`