ANNALES MATHÉMATIQUES

BLAISE PASCAL

Yasuhiro Kishi

On D_5-polynomials with integer coefficients

Volume 16, n^o 1 (2009), p. 113-125.

<http://ambp.cedram.org/item?id=AMBP_2009__16_1_113_0>

Publication éditée par le laboratoire de mathématiques
de l'université Blaise-Pascal, UMR 6620 du CNRS
Clermont-Ferrand — France

Annales mathématiques Blaise Pascal **16**, 113-125 (2009)

On D_5-polynomials with integer coefficients

Yasuhiro Kishi

Abstract

We give a family of D_5-polynomials with integer coefficients whose splitting fields over $\mathbf{Q}$ are unramified cyclic quintic extensions of quadratic fields. Our polynomials are constructed by using Fibonacci, Lucas numbers and units of certain cyclic quartic fields.

1. Introduction

The following is a fundamental problem in the theory of quadratic fields: For a given positive integer N, find quadratic fields whose class number is divisible by N. Several authors (for example, T. Nagell [6], N. C. Ankeny and S. Chowla [1], Y. Yamamoto [12], P. J. Weinberger [11] and H. Ichimura [3]) gave an infinite family of quadratic fields whose class number is divisible by arbitrary given integer N. If limited to the case $N = 5$, C. J. Parry [8], J.-F. Mestre [5], M. Sase [10] and D. Byeon [2] gave a family of quadratic fields whose class number is divisible by 5. In particular, Sase [10] gave a family of polynomials whose splitting field is a D_5-extension of $\mathbf{Q}$ and an unramified C_5-extension of containing the quadratic field. In the present paper, we will give other such polynomials by the use of the result of our previous result [4]. Then we get a new family of quadratic fields whose class number is divisible by 5. As a consequence, the following conjecture arises:

Conjecture 1.1. *Let F_n denote the n-th number in the Fibonacci sequence:*

$$1, 1, 2, 3, 5, 8, 13, \dots$$

Then the class number of the quadratic field $\mathbf{Q}(\sqrt{-F_{50s+25}})$ $(s \geq 0)$ is divisible by 5*.*

Keywords: class number, Fibonacci number, polynomial.
Math. classification: 11R29.

The organization of this paper is as follows. In Section 1, we state the main theorem that the above conjecture is true under some conditions. In Section 2, we give a parametric D_5-polynomial with integer coefficients. It is a review of [4]. In Section 3, we study the Fibonacci and the Luca sequences. In Section 4, we give a proof of the main theorem. We give a numerical example in the last Section 5.

We list here those symbols which will be used throughout this article.

Let $\mathbf{Q}$ denote the field of rational numbers and $\mathbf{Z}$ denote the ring of rational integers.

For an integer n, let C_n and D_n denote the cyclic group of order n and the dihedral group of order $2n$, respectively.

For an extension L/K, denote the norm map and the trace map of L/K by $N_{L/K}$ and by $\mathrm{Tr}_{L/K}$, respectively. For simplicity, we denote N_L and Tr_L if the base field $K = \mathbf{Q}$. For a Galois extension L/K, we denote the Galois group of L/K by $\mathrm{Gal}(L/K)$.

For a polynomial $f(X)$ and a field K, we denote the minimal splitting field of $f(X)$ over K by $\mathrm{Spl}_K(f)$.

2. The main Theorem

To state the main theorem, we prepare some notations.

Let (F_n) and (L_n) be the Fibonacci and the Luca sequences, respectively, defined as follows:

$$F_1 = 1, \quad F_2 = 1, \quad F_{n+2} = F_{n+1} + F_n \ (n \geq 1),$$
$$L_1 = 1, \quad L_2 = 3, \quad L_{n+2} = L_{n+1} + L_n \ (n \geq 1).$$

Let $\zeta := e^{2\pi i/5}$ be a primitive fifth root of unity. For a non-negative integer m, we set $k_m := \mathbf{Q}(\sqrt{-F_{2m+1}})$. Moreover we define a cyclic quartic field M_m as follows: M_m is the proper subextension of $k_m(\zeta)/\mathbf{Q}(\sqrt{5})$ other than $k_m(\sqrt{5})$ and $\mathbf{Q}(\zeta)$. Then we can express $M_m = \mathbf{Q}(\sqrt{-F_{2m+1}}(\zeta - \zeta^{-1}))$. We define an element δ_m of M_m by

$$\delta_m := 1 + \varepsilon^m \sqrt{-F_{2m+1}}(\zeta - \zeta^{-1}),$$

where $\varepsilon := (1+\sqrt{5})/2$ is a fundamental unit of $\mathbf{Q}(\sqrt{5})$. As we will see in Section 4, δ_m is a unit in M_m. Let τ be a generator of $\mathrm{Gal}(k_m(\zeta)/k_m)$ ($\cong C_4$) with $\zeta^\tau = \zeta^2$.

For a non-negative integer m, we define a polynomial $g_m(X)$ of degree 5 with integer coefficients by

$$g_m(X) := X^5 - 10X^3 - 20X^2 + 5(20F_{2m+1}^2 - 3)X \\ + 40F_{2m+1}^2((-1)^m L_{2m+1} + 1) - 4.$$

Under the above notations and assumptions, we have the following.

Theorem 2.1. *Let m be a non-negative integer. If $\delta_m^{2+3\tau+\tau^2}$ is not a fifth power in M_m, then $\mathrm{Spl}_{\mathbf{Q}}(g_m)$ is a D_5-extension of $\mathbf{Q}$ containing k_m. If, moreover, $m \equiv 12 \pmod{5^2}$, then $\mathrm{Spl}_{\mathbf{Q}}(g_m)$ is an unramified cyclic quintic extension of k_m. Hence, by putting $m = 25s + 12$, the class number of the quadratic field $\mathbf{Q}(\sqrt{-F_{50s+25}})$ is divisible by 5.*

Remarks 2.2. The author think the assumption "$\delta_m^{2+3\tau+\tau^2}$ is not a fifth power in M_m" can be excluded (cf. Remark 6.2).

3. Construction of D_5-polynomials

This section is a review of [4] in the case $p = 5$ and the base field $\mathbf{Q}$. Let ζ be a primitive fifth root of unity, and let $k = \mathbf{Q}(\sqrt{D})$ be a quadratic field which does not coincide with $\mathbf{Q}(\sqrt{5})$. Then there exists a unique proper subextension of the bicyclic biquadratic extension $k(\zeta)/\mathbf{Q}(\sqrt{5})$ other than $k(\sqrt{5})$ and $\mathbf{Q}(\zeta)$. We denote it by M. Then M is a cyclic quartic field. Let us call M *the associated field with k*. Fix the generator τ of $\mathrm{Gal}(k(\zeta)/k)$ with $\zeta^\tau = \zeta^2$, and define a subset $\mathcal{M}(k)$ of $k(\zeta)^\times$ as follows:

$$\mathcal{M}(k) := \{\gamma \in k(\zeta)^\times \mid \gamma^{3+4\tau+2\tau^2+\tau^3} \notin k(\zeta)^5\}.$$

For an element $\gamma \in M$, we define a polynomial $f_\gamma(X)$ by

$$f_\gamma(X) := X^5 - 10N_M(\gamma)X^3 - 5N_M(\gamma)NT(\gamma)X^2 \\ + 5N_M(\gamma)\{N_M(\gamma) - NT(\gamma^{1+\tau})\}X - N_M(\gamma)NT(\gamma^{2+\tau}),$$

where $NT = N_{\mathbf{Q}(\sqrt{5})}\mathrm{Tr}_{M/\mathbf{Q}(\sqrt{5})}$.

Applying [4, Theorem 2.1, Corollary 2.6] to the case $p = 5$, we get the following proposition.

Proposition 3.1. *Let the notation be as above. Then for $\delta \in \mathcal{M}(k) \cap M$, $\mathrm{Spl}_{\mathbf{Q}}(f_\delta)$ is a D_5-extension of $\mathbf{Q}$ containing k. Putting $E := \mathrm{Spl}_{\mathbf{Q}}(f_\delta)$,* *moreover, we have*

$$E = k\Big(\mathrm{Tr}_{E(\zeta)/E}\big(\sqrt[5]{\delta^{3+4\tau+2\tau^2+\tau^3}}\big)\Big).$$

Remarks 3.2. In [4], we can see that every D_5-extension E of $\mathbf{Q}$ containing k is given as $E = \mathrm{Spl}_{\mathbf{Q}}(f_\delta)$ for some $\delta \in \mathcal{M}(k) \cap M$.

4. Properties of Fibonacci and Lucas numbers

There are many relations between Fibonacci and Lucas numbers. (See for example [9] and [7].) In this section, we show the following four properties which we need in the next section.

(A) The power of $\varepsilon = (1+\sqrt{5})/2$ is expressed by

$$\varepsilon^m = \frac{L_m + F_m\sqrt{5}}{2}.$$

(B) For positive integer m, we have

$$F_{m+1} = \frac{L_m + F_m}{2}, \tag{4.1}$$

$$L_{m+1} = \frac{L_m + 5F_m}{2}. \tag{4.2}$$

(C) Let m be a positive integer. If m is divisible by 5^2, then so is F_m.

(D) Let n and m be positive integers. If $d = \gcd(n, m)$, then we have

$$\gcd(F_n, F_m) = F_d.$$

We easily get the property (A) by mathematical induction on m, using

$$\begin{aligned}\varepsilon^{m+1} &= \frac{L_m + F_m\sqrt{5}}{2} \cdot \frac{1+\sqrt{5}}{2}\\ &= \frac{(L_m + 5F_m)/2 + (L_m + F_m)/2 \cdot \sqrt{5}}{2},\end{aligned}$$

and the property (B).

We will prove the property (B) by mathematical induction on m. The equations (4.1) and (4.2) hold clearly for $m = 1$. Assume that (4.1) and

(4.2) hold for m. Then we have

$$\begin{aligned}\frac{L_{m+1}+F_{m+1}}{2} &= \frac{(L_m+5F_m)/2+F_{m+1}}{2} = \frac{L_m+5F_m+2F_{m+1}}{4}\\ &= \frac{(2F_{m+1}-F_m)+5F_m+2F_{m+1}}{4} = F_{m+1}+F_m = F_{m+2}\end{aligned}$$

and

$$\begin{aligned}\frac{L_{m+1}+5F_{m+1}}{2} &= \frac{L_{m+1}+5(L_m+F_m)/2}{2} = \frac{2L_{m+1}+5L_m+5F_m}{4}\\ &= \frac{2L_{m+1}+5L_m+(2L_{m+1}-L_m)}{4} = L_{m+1}+L_m = L_{m+2}.\end{aligned}$$

Hence (4.1) and (4.2) hold for $m+1$.

Before proving the property (C), we show that the relation

$$F_{n+m} = F_mF_{n+1} + F_{m-1}F_n \tag{4.3}$$

holds for positive integers n, m. For any n, we have

$$\begin{aligned}F_{n+1} &= 1\cdot F_{n+1} + 0\cdot F_n = F_1F_{n+1} + F_0F_n,\\ F_{n+2} &= 1\cdot F_{n+1} + 1\cdot F_n = F_2F_{n+1} + F_1F_n.\end{aligned}$$

(For convenience we define $F_0 = 0$.) Then (4.3) holds for $m = 1, 2$. Assume that (4.3) holds for $m = k$, $k-1$:

$$\begin{aligned}F_{n+k} &= F_kF_{n+1} + F_{k-1}F_n,\\ F_{n+(k-1)} &= F_{k-1}F_{n+1} + F_{k-2}F_n.\end{aligned}$$

Then we have

$$\begin{aligned}F_{n+(k+1)} &= F_{n+k} + F_{n+(k-1)}\\ &= (F_kF_{n+1} + F_{k-1}F_n) + (F_{k-1}F_{n+1} + F_{k-2}F_n)\\ &= (F_k + F_{k-1})F_{n+1} + (F_{k-1} + F_{k-2})F_n = F_{k+1}F_{n+1} + F_kF_n.\end{aligned}$$

Hence (4.3) holds for $m = k+1$.

Next we prove

$$m \equiv 0 \pmod{n} \implies F_m \equiv 0 \pmod{F_n}, \tag{4.4}$$

namely,

$$F_{nk} \equiv 0 \pmod{F_n}$$

for each $k \in \mathbf{Z}$, $k \geq 1$. It holds clearly for $k = 1$. Assume that $F_{nk} \equiv 0 \pmod{F_n}$. Then by (4.3), we have

$$F_{n(k+1)} = F_{nk+n} = F_n F_{nk+1} + F_{n-1} F_{nk} \equiv 0 \pmod{F_n}.$$

Hence (4.4) is proved.

The property (C) follows from (4.4) and $F_{25} = 75025 \equiv 0 \pmod{5^2}$.

For positive integers n and m, express $n = qm + r$, $0 \leq r \leq m$. Then we claim

$$\gcd(F_n, F_m) = \gcd(F_r, F_m). \tag{4.5}$$

Using (4.3) and (4.4), we have

$$\begin{aligned} \gcd(F_n, F_m) &= \gcd(F_{qm+r}, F_m) \\ &= \gcd(F_{qm} F_{r+1} + F_{qm-1} F_r, F_m) \\ &= \gcd(F_{qm-1} F_r, F_m). \end{aligned}$$

Here we have

$$\begin{aligned} \gcd(F_{qm-1}, F_{qm}) &= \gcd(F_{qm-1}, F_{qm-1} + F_{qm-2}) = \gcd(F_{qm-1}, F_{qm-2}) \\ &= \cdots\cdots = \gcd(F_2, F_1) = \gcd(1, 1) = 1. \end{aligned}$$

From this together with $F_m \mid F_{qm}$, we have $\gcd(F_{qm-1}, F_m) = 1$. Then we get (4.5). Hence by using the Euclidean algorithm, the property (D) follows.

Remarks 4.1. The inverse of the property (C) also holds true.

5. **Proof of the main theorem**

The goal of this section is to give a proof of our main theorem.

By the definition, M_m is the associated field with k_m. Hence we can apply Proposition 3.1. Now let us calculate $f_{\delta_m}(X)$;

$$\begin{aligned} f_{\delta_m}(X) = X^5 &- 10 N_M(\delta_m) X^3 - 5 N_M(\delta_m) NT(\delta_m) X^2 \\ &+ 5 N_M(\delta_m)\{N_M(\delta_m) - NT(\delta_m^{1+\tau})\} X - N_M(\delta_m) NT(\delta_m^{2+\tau}). \end{aligned}$$

We note that τ satisfies the following:

$$\zeta^\tau = \zeta^2, \quad (\sqrt{5})^\tau = -\sqrt{5}, \quad (\sqrt{-F_{2m+1}})^\tau = \sqrt{-F_{2m+1}}.$$

Put $\overline{\varepsilon} := \varepsilon^\tau$; then we have

$$\begin{aligned}
N_M(\delta_m) &= (1+\varepsilon^m\sqrt{-F_{2m+1}}(\zeta-\zeta^{-1}))(1+\overline{\varepsilon}^m\sqrt{-F_{2m+1}}(\zeta^2-\zeta^{-2}))\\
&\quad \times (1-\varepsilon^m\sqrt{-F_{2m+1}}(\zeta-\zeta^{-1}))(1-\overline{\varepsilon}^m\sqrt{-F_{2m+1}}(\zeta^2-\zeta^{-2}))\\
&= (1+\varepsilon^{2m}F_{2m+1}(\zeta-\zeta^{-1})^2)(1+\overline{\varepsilon}^{2m}F_{2m+1}(\zeta^2-\zeta^{-2})^2)\\
&= \left(1-\frac{5+\sqrt{5}}{2}\varepsilon^{2m}F_{2m+1}\right)\left(1-\frac{5-\sqrt{5}}{2}\overline{\varepsilon}^{2m}F_{2m+1}\right)\\
&= 1-\frac{5+\sqrt{5}}{2}\varepsilon^{2m}F_{2m+1}-\frac{5-\sqrt{5}}{2}\overline{\varepsilon}^{2m}F_{2m+1}\\
&\quad + 5N_{\mathbf{Q}(\sqrt{5})}(\varepsilon)^{2m}F_{2m+1}^2\\
&= 1-F_{2m+1}\left\{\mathrm{Tr}_{\mathbf{Q}(\sqrt{5})}\left(\frac{5+\sqrt{5}}{2}\varepsilon^{2m}\right)-5F_{2m+1}\right\},
\end{aligned}$$

by using

$$(\zeta-\zeta^{-1})^2 = \left(2i\sin\frac{2\pi}{5}\right)^2 = -\frac{5+\sqrt{5}}{2}$$

and

$$(\zeta^2-\zeta^{-2})^2 = \left(2i\sin\frac{4\pi}{5}\right)^2 = -\frac{5-\sqrt{5}}{2}.$$

Here, by (4.1) we have

$$\begin{aligned}
\mathrm{Tr}_{\mathbf{Q}(\sqrt{5})}\left(\frac{5+\sqrt{5}}{2}\varepsilon^{2m}\right) &= \mathrm{Tr}_{\mathbf{Q}(\sqrt{5})}\left(\frac{5+\sqrt{5}}{2}\cdot\frac{L_{2m}+F_{2m}\sqrt{5}}{2}\right)\\
&= \frac{5L_{2m}+5F_{2m}}{2}\\
&= 5F_{2m+1}.
\end{aligned}$$

Therefore we get $N_M(\delta_m)=1$. By similar calculations, we have

$$\begin{aligned}
NT(\delta_m) &= 4,\\
NT(\delta_m^{1+\tau}) &= 4-20F_{2m+1}^2,\\
NT(\delta_m^{2+\tau}) &= 4-40F_{2m+1}^2(1+(-1)^nL_{2m+1}).
\end{aligned}$$

Substituting them into $f_{\delta_m}(X)$, we have

$$\begin{aligned} f_{\delta_m}(X) &= X^5 - 10X^3 - 20X^2 + 5(20F_{2m+1}^2 - 3)X \\ &\quad + 40F_{2m+1}^2((-1)^n L_{2m+1} + 1) - 4 \\ &= g_m(X). \end{aligned}$$

Assume that $\delta_m^{2+3\tau+\tau^2}$ is not a fifth power in M_m. Then we have

$$\delta_m^{3+4\tau+2\tau^2+\tau^3} = N_M(\delta_m)\delta_m^{2+3\tau+\tau^2} = \delta_m^{2+3\tau+\tau^2} \notin k_m(\zeta)^5,$$

and hence $\delta_m^{3+4\tau+2\tau^2+\tau^3} \in \mathcal{M}(k_m)$. Then by Proposition 3.1, $\mathrm{Spl}_{\mathbf{Q}}(g_m)$ $(= \mathrm{Spl}_{\mathbf{Q}}(f_{\delta_m}))$ is a D_5-extension of $\mathbf{Q}$ containing k_m.

Assume in addition that $m \equiv 12 \pmod{5^2}$. We will show that the cyclic quintic extension $\mathrm{Spl}_{\mathbf{Q}}(g_m)/k_m$ is unramified. Let θ be a root of $g_m(X)$. Let q be a prime number in general. A prime divisor of q in k_m is ramified in $\mathrm{Spl}_{\mathbf{Q}}(g_m)$ if and only if q is totally ramified in $\mathbf{Q}(\theta)$ because $[\mathrm{Spl}_{\mathbf{Q}}(g_m) : k_m]$ and $[k_m : \mathbf{Q}]$ are relatively prime. Hence we have only to verify that no primes are totally ramified in $\mathbf{Q}(\theta)$. This can be proved by using the following Sase's result. For a prime number p and for an integer m, we denote the greatest exponent μ of p such that $p^\mu \mid m$ by $v_p(m)$.

Proposition 5.1. [10, Proposition 2] *Let p $(\neq 2)$ and q be prime numbers. Suppose that the polynomial*

$$\varphi(X) = X^p + \sum_{j=0}^{p-2} a_j X^j, \quad a_j \in \mathbf{Z}$$

is irreducible over $\mathbf{Q}$ and satisfies the condition

$$v_q(a_j) < p - j \quad \textit{for some } j,\ 0 \leq j \leq p-2. \tag{5.1}$$

Let θ be a root of $\varphi(X)$.
(1) If q is different from p, then q is totally ramified in $\mathbf{Q}(\theta)/\mathbf{Q}$ if and only if

$$0 < \frac{v_q(a_0)}{p} \leq \frac{v_q(a_j)}{p-j} \quad \textit{for every } j,\ 1 \leq j \leq p-2.$$

(2) *The prime p is totally ramified in $\mathbf{Q}(\theta)/\mathbf{Q}$ if and only if one of the following conditions* (S-i), (S-ii) *holds*:

(S-i) $0 < \dfrac{v_p(a_0)}{p} \leq \dfrac{v_p(a_j)}{p-j}$ *for every j*, $1 \leq j \leq p-2$;

(S-ii) (S-ii-1) $v_p(a_0) = 0$,

(S-ii-2) $v_p(a_j) > 0$ *for every j*, $1 \leq j \leq p-2$,

(S-ii-3) $\dfrac{v_p(\varphi(-a_0))}{p} \leq \dfrac{v_p(\varphi^{(j)}(-a_0))}{p-j}$ *for every j*, $1 \leq j \leq p-2$,

and

(S-ii-4) $v_p(\varphi^{(j)}(-a_0)) < p-j$ *for some j*, $0 \leq j \leq p-1$,

where $\varphi^{(j)}(X)$ is the j-th differential of $\varphi(X)$.

Now let us apply Proposition 4.1 to our polynomial $g_m(X)$. First, we easily verify that $g_m(X)$ satisfies (4.1) for each prime. Next, we see from Proposition 4.1 (1) that no primes except for 5 are totally ramified in $\mathbf{Q}(\theta)/\mathbf{Q}$ because the greatest common divisor of the coefficient of X^3 and that of X is equal to 5. We will show, therefore, that 5 is not totally ramified. Denote the constant term of $g_m(X)$ by c_0;

$$c_0 := 40F_{2m+1}^2((-1)^n L_{2m+1} + 1) - 4.$$

Since c_0 is not divisible by 5, the condition (S-i) does not hold. By the assumption $m \equiv 12 \pmod{5^2}$, we have $2m+1 \equiv 0 \pmod{5^2}$. Then by the property (C), in Section 3, we have $F_{2m+1} \equiv 0 \pmod{5^2}$, and hence $-c_0 \equiv 4 \pmod{5^5}$. Therefore we have

$$\begin{aligned}
g_m(-c_0) &\equiv 4^5 - 10\cdot 4^3 - 20\cdot 4^2 - 5(20d^2-3)\cdot 4 - 4 \equiv 0 \pmod{5^5},\\
g_m^{(1)}(-c_0) &\equiv 5\cdot 4^4 - 30\cdot 4^2 - 40\cdot 4 - 15 \equiv 0 \pmod{5^4},\\
g_m^{(2)}(-c_0) &\equiv 20\cdot 4^3 - 60\cdot 4^2 - 40 \equiv 0 \pmod{5^3},\\
g_m^{(3)}(-c_0) &\equiv 60\cdot 4^2 - 60 \equiv 0 \pmod{5^2}.
\end{aligned}$$

Then the condition (S-ii-4) does not hold. (We can easily check that (S-ii-1), (S-ii-2) and (S-ii-3) hold.) Hence 5 is not totally ramified in $\mathbf{Q}(\theta)$. This completes the proof of the main theorem.

Next, we consider when $\delta_m^{2+3\tau+\tau^2}$ is not a fifth power in M_m.

Suppose that $\delta_m^{2+3\tau+\tau^2}$ is a fifth power in M_m; $\delta_m^{2+3\tau+\tau^2} = \alpha^5$, $\alpha \in M_m$. Since

$$\delta_m^{3+4\tau+2\tau^2+\tau^3} = N_M(\delta_m)\delta_m^{2+3\tau+\tau^2} = \delta_m^{2+3\tau+\tau^2} = \alpha^5$$

and M_m is normal over $\mathbf{Q}$, we have

$$\mathrm{Tr}_{E(\zeta)/E}\Big(\sqrt[5]{\delta_m^{3+4\tau+2\tau^2+\tau^3}}\Big) = \mathrm{Tr}_{E(\zeta)/E}(\alpha) \in M_m,$$

where $E = \mathrm{Spl}_{\mathbf{Q}}(g_m)$. By the last half of Proposition 3.1, therefore, we have

$$\mathrm{Spl}_{\mathbf{Q}}(g_m) = k_m(\mathrm{Tr}_{E(\zeta)/E}(\alpha)) \subset M_m.$$

Hence the degree $[\mathrm{Spl}_{\mathbf{Q}}(g_m) : k_m]$ is less than 5. Then $g_m(X)$ must be reducible over $\mathbf{Q}$. Therefore, we have

Proposition 5.2. *The element $\delta_m^{2+3\tau+\tau^2}$ is not a fifth power in M_m if and only if $g_m(X)$ is irreducible over $\mathbf{Q}$.*

Finally in this section, we prove the following.

Proposition 5.3. *The set*

$$\Big\{\mathbf{Q}(\sqrt{-F_{50s+25}})\,\Big|\, s \geq 0\Big\}$$

is infinite.

Proof. On the contrary, we assume $\#\{\mathbf{Q}(\sqrt{-F_{50s+25}}) \mid s \geq 0\} < \infty$. For an integer m, we denote the square free part of m by $\mathrm{sf}(m)$. By the assumption, the set

$$\mathcal{P} := \bigcup_{s \geq 0}\{\text{prime factors of } \mathrm{sf}(F_{50s+25})\}$$

is finite. Then there exists a positive integer t so that we have

$$\mathcal{P} = \bigcup_{0 \leq s \leq t}\{\text{prime factors of } \mathrm{sf}(F_{25(2s+1)})\}.$$

Take a prime q with $q > 2t+1$. Then for each prime factor r of $\mathrm{sf}(F_{25q})$, we have

$$\mathrm{sf}(F_{25(2s+1)}) \equiv 0 \pmod{r} \quad \text{for some } s,\ 0 \leq s \leq t. \tag{5.2}$$

On the other hand, because q is prime, for each s, $0 \leq s \leq t$, we have

$$\gcd(25(2s+1), 25q) = 25,$$

and hence by the property (D),

$$\gcd(F_{25(2s+1)}, F_{25q}) = F_{25} = 3001 \cdot 5^2.$$

From this together with (5.2), we can express

$$F_{25q} = 3001 A_q^2$$

for some $A_q \in \mathbf{Z}$. Then we have

$$-1 = N_{\mathbf{Q}(\sqrt{5})}(\varepsilon^{25q}) = \frac{L_{25q}^2 - 5F_{25q}^2}{4} = \frac{L_{25q}^2 - 5 \cdot 3001^2 A_q^4}{4}$$

This implies that (A_q, L_{25q}) is an integer solution of the equation

$$Y^2 = 5 \cdot 3001^2 X^4 - 4. \tag{5.3}$$

The values of L_{25q} (q is prime), of course, are different from each other. However by Siegel's theorem, there are only finitely many integer solutions (X, Y) of Eq. (5.3), This is a contradiction. □

6. Numerical examples

Example 6.1. Let $m = 12$. By $F_{12} = 144$, $L_{12} = 322$ and $F_{25} = 3001 \cdot 5^2$, we have

$$\delta_{12} = 1 + \frac{322 + 144\sqrt{5}}{2}\sqrt{-3001 \cdot 5^2}(\zeta - \zeta^{-1})$$

and $g_{12}(X) = f_{\delta_{12}}(X)$ is given by

$$X^5 - 10X^3 - 20X^2 + 562875062485X + 37771618494049996.$$

Since $g_{12}(X)$ is irreducible over $\mathbf{Q}$, it follows from Proposition 5.2 that δ_{12} is not a fifth power in M_m. Then by the main theorem, the splitting field of $g_{12}(X)$ is an unramified cyclic quintic extension of $\mathbf{Q}(\sqrt{-F_{25}})$.

In the following table, we list the prime decompositions of $-F_{2m+1}$ and the structure of the ideal class groups of $k_m = \mathbf{Q}(\sqrt{-F_{2m+1}})$ for $m \leq 87$ with $m \equiv 12 \pmod{5^2}$.

Remarks 6.2. For this table we use GP/PARI (Version 2.1.5). By using the same calculator, the author verified that $g_m(X)$ is irreducible over $\mathbf{Q}$ for every m, $0 \leq m \leq 2000$. (The disit of the constant term of $g_{2000}(X)$ is 2510.)

m	$-F_{2m+1}$	Structure of the ideal class group of $k_m = \mathbf{Q}(\sqrt{-F_{2m+1}})$
12	$-3001 \cdot 5^2$	C_{40}
37	$-2 \cdot 61 \cdot 3001 \cdot 230686501 \cdot 5^2$	$C_{2461460} \times C_2 \times C_2$
62	$-5 \cdot 3001 \cdot 158414167964045700001 \cdot 5^2$	$C_{79285156360} \times C_8 \times C_2$
87	$-13 \cdot 701 \cdot 3001 \cdot 141961$ $\times 172312037302011893083 01 \cdot 5^2$	$C_{1737032019043290}$ $\times C_6 \times C_2 \times C_2 \times C_2$

Acknowledgments

The author is grateful to Abdelmalek Azizi, Mohammed Ayadi, Moulay C. Ismaili and their colleagues for their kind hospitality during the conference *Congrès International Algèbre, Théorie des Nombres et leurs Applications.* Together, they made it possible to spend a wonderful week in Morocco.

Added in proof

After this paper had been written, the author proved our conjecture (Conjecture 1.1) himself. For the details, see in "A new family of imaginary quadratic fields whose class number is divisible by five", J. Number Theory **128** (2008), 2450–2458.

References

[1] N. C. Ankeny and S. Chowla, *On the divisibility of the class number of quadratic fields*, Pacific J. Math. **5** (1955), 321–324. MR MR0085301 (19,18f)

[2] Dongho Byeon, *Real quadratic fields with class number divisible by 5 or 7*, Manuscripta Math. **120** (2006), no. 2, 211–215. MR MR2234249 (2007f:11124)

[3] H. Ichimura, *Note on the class numbers of certain real quadratic fields*, Abh. Math. Sem. Univ. Hamburg **73** (2003), 281–288. MR MR2028521 (2004k:11174)

[4] Masafumi Imaoka and Yasuhiro Kishi, *On dihedral extensions and Frobenius extensions*, Galois theory and modular forms, Dev. Math., vol. 11, Kluwer Acad. Publ., Boston, MA, 2004, pp. 195–220. MR MR2059764 (2005f:11245)

[5] Jean-François Mestre, *Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques*, J. Reine Angew. Math. **343** (1983), 23–35. MR MR705875 (84m:12004)

[6] T. Nagell, *Über die Klassenzahl imaginär-quadratischer Zahlköper*, Abh. Math. Sem. Univ. Hamburg **1** (1922), 140–150.

[7] S. Nakamura, *A microcosm of fibonacci numbers (japanese)*, Nippon Hyoronsha Co., Tokyo, 2002.

[8] Charles J. Parry, *On the class number of relative quadratic fields*, Math. Comp. **32** (1978), no. 144, 1261–1270. MR MR502013 (80h:12004)

[9] Paulo Ribenboim, *The new book of prime number records*, Springer-Verlag, New York, 1996. MR MR1377060 (96k:11112)

[10] Masahiko Sase, *On a family of quadratic fields whose class numbers are divisible by five*, Proc. Japan Acad. Ser. A Math. Sci. **74** (1998), no. 7, 120–123. MR MR1658854 (2000b:11117)

[11] P. J. Weinberger, *Real quadratic fields with class numbers divisible by n*, J. Number Theory **5** (1973), 237–241. MR MR0335471 (49 #252)

[12] Yoshihiko Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. **7** (1970), 57–76. MR MR0266898 (42 #1800)

Yasuhiro Kishi
Department of Mathematics
Fukuoka University of Education
1-1 Bunkyoumachi Akama, Munakata-shi
Fukuoka, 811-4192
Japan
ykishi@fukuoka-edu.ac.jp