On a system of norm-equations over cyclic cubic number fields.

Attila Pethő*
Laboratory for Computer Science
University Medical School Debrecen
Nagyerdei krt. 98
H-4028 Debrecen, Hungary
Horst G. Zimmer
Fachbereich 9 Mathematik
Universität des Saarlandes
D-66041 Saarbrücken, Germany

November 28, 2009

1 Introduction and the Theorem

In [7] we determined all torsion groups of elliptic curves with integral $j-$invariant over arbitrary cubic fields. We found in particular, that there are infinitely many curves having a torsion group isomorphic to $\mathbb{Z}/5\mathbb{Z}$. Moreover we obtained a parametrization for the defining polynomials of the possible cubic ground fields. Using this parametrization we proved that, in contrast to the general case, there are only finitely many curves having a torsion group isomorphic to $\mathbb{Z}/5\mathbb{Z}$ over *cyclic* cubic fields. The proof is based on the Theorem below already mentioned (but not proved) in [6]. Here we shall provide a detailed proof of that theorem, where we shall use ideas of [1], [2], [5] and [8].

Theorem 1 *Let $n \geq 0$ be an integer, $\varepsilon, \varepsilon_1 \in \{1, -1\}$ and denote by $\mathbb{K}$ a cyclic cubic number field. Assume that there exist an $\eta \in \mathbb{Z}_{\mathbb{K}}$, the ring of integers of $\mathbb{K}$, such that*

$$N_{\mathbb{K}/\mathbf{Q}}(\eta) \quad = \quad \varepsilon \tag{1}$$

*Research partially supported by Hungarian National Foundation for Scientific Research Grant No 16791/95.

$$N_{\mathbb{K}/\mathbf{Q}}(\eta^2 - 11\eta - 1) \quad = \quad \varepsilon_1 5^n.$$

Then $\mathbb{K}$ is generated by a zero of one of the following eight polynomials p (for which the discriminants of p and $\mathbb{K}$ are also listed).

i	$p(z)$	$D(p(z))$	$D_{\mathbb{K}}$	n
1	$z^3 - 12z^2 + 9z + 1$	$(3^2 \cdot 13)^2$	$(3^2 \cdot 13)^2$	*0*
2	$z^3 - 12z^2 + 35z + 1$	$(5 \cdot 13)^2$	13^2	*4*
3	$z^3 + 3z^2 - 160z + 1$	$(5^2 \cdot 163)^2$	163^2	*4*
4	$z^3 - 17z^2 - 25z + 1$	$(2^3 \cdot 5 \cdot 13)^2$	13^2	*5*
5	$z^3 - 13z^2 + 10z + 1$	139^2	139^2	*0*
6	$z^3 - 14z^2 + 11z + 1$	163^2	163^2	*2*
7	$z^3 - 9z^2 + 6z + 1$	$(3^2 \cdot 7)^2$	$(3^2 \cdot 7)^2$	*3*
8	$z^3 + 3z^2 - 10z + 1$	$(5 \cdot 13)^2$	13^2	*5*

Moreover if $\eta \in \mathbb{Z}_{\mathbb{K}}$ is a solution of (1) then either η or $-1/\eta$ is a zero of the generating polynomial p of $\mathbb{K}$.

2 Auxiliary Results

In the sequel we denote by $\{F_n\}_{-\infty}^{\infty}$ and $\{L_n\}_{-\infty}^{\infty}$ the sequence of the Fibonacci and Lucas numbers respectively. They are given by the initial conditions $F_0 = 0, F_1 = 1$ and $L_0 = 2, L_1 = 1$ and satisfy the difference equation

$$x_{n+1} = x_n + x_{n-1}.$$

For later application, we list several properties of these sequences.

(P1) If $x, y \in \mathbb{Z}$ is a solution of the diophantine equation

$$x^2 - 5y^2 = \pm 4$$

then $(x, y) = (\pm L_m, \pm F_m)$ for some integer $m \in \mathbb{Z}_{\geq 0}$.

(P2)

$$F_{-n} = \begin{cases} F_n, & \text{if } n \text{ is odd} \\ -F_n, & \text{if } n \text{ is even} \end{cases}$$

and

$$L_{-n} = \begin{cases} -L_n, & \text{if } n \text{ is odd} \\ L_n, & \text{if } n \text{ is even} \end{cases}$$

(P3) $2F_{n+m} = F_m L_n + F_n L_m$

(P4) $2L_{n+m} = L_m L_n + 5F_m F_n$

(P5) Let $n = \pm 2^\alpha \cdot 3^\beta \cdot k$ for $\alpha, \beta \in \mathbb{Z}_{\geq 0}$ with $\alpha \geq 2$ and $k \in \mathbb{Z}$ such that $gcd(k, 6) = 1$. Then for any $m \in \mathbb{Z}$
$F_{n+m} \equiv -F_m \pmod{L_{2^{\alpha-2}k}}$ and
$L_{n+m} \equiv -L_m \pmod{L_{2^{\alpha-2}k}}$.

(P6) For any $M \in \mathbb{N}$, the sequences $\{F_m \bmod M\}_{-\infty}^{\infty}$ and $\{L_m \bmod M\}_{-\infty}^{\infty}$ are periodic.
The minimal length of period of the corresponding sequence will be denoted by $r(M) = r_F(M)$ and $r_L(M)$. We have $r_L(M) | r_F(M)$.

(P7) $5|F_n$ if and only if $5|n$.

(P8) If $k \in \mathbb{N}$ is odd, then $L_n | L_{kn}$ for any $n \in \mathbb{Z}$.

(P9) For any $m \in \mathbb{Z}$, $L_{2m} = L_m^2 - 2(-1)^m$

Using the properties of the Fibonacci and Lucas numbers listed above we first characterize the solutions of (1) in cubic fields.

Lemma 1 *Let $\varepsilon = -1$, $\mathbb{K}$ a cubic number field and $\eta \in \mathbb{Z}_{\mathbb{K}}$ a solution of (1). Then there exist an $m \in \mathbb{Z}_{\geq 0}$ and $\varepsilon_2, \varepsilon_3 \in \{1, -1\}$ such that η is a zero of the polynomial*

$$P(z) := P(z; k, m, \varepsilon_2, \varepsilon_3) = z^3 + (-12 + \varepsilon_2 5^k G_m) z^2 + (10 + \varepsilon_2 \varepsilon_3 5^k G_{m-5\varepsilon_3}) z + 1,$$

where

$$G_m = \begin{cases} F_m & , \text{ if } n = 2(k+1), \ \ k \in \mathbb{Z}_{\geq 0} \\ L_m & , \text{ if } n = 2(k+1)+1, \ \ k \in \mathbb{Z}_{\geq 0} \\ F_{5m} & , \text{ if } n = 0, \ \ k = -1. \end{cases}$$

For $n = 1$, (1) is unsolvable.

Conversely, is η is a zero of the polynomial $P(z; k, m, \varepsilon_2, \varepsilon_3)$ and $\mathbb{K} = \mathbf{Q}(\eta)$, then η is a solution of (1) in $\mathbb{Z}_{\mathbb{K}}$.

Remarks

(a.) It follows immediately from Lemma 1 that for any $n \in \mathbb{Z}_{\geq 0}$, $n \neq 1$, there exit infinitely many cubic fields in which (1) is solvable.

(b.) Let us fix a cubic number field $\mathbb{K}$ and consider the extension field $L = \mathbb{K}(\sqrt{5})$. By the same argument as in Fung et al. [3], one can easily show that n is bounded and (1) has only finitely many effectively computable solutions $\eta \in \mathbb{Z}_{\mathbb{K}}$. But their method seems not capable to show that there exists only finitely many cyclic cubic fields, for which (1) is solvable.

The Lemma could be proved by using the Theorem of [6] but we prefer to argue here directly.

Proof of Lemma 1. Suppose that $\eta \in \mathbb{Z}_{\mathbb{K}}$ solves (1). Let $P(x) = z^3 - vz^2 + m_1 z + 1$ and $q(z)$ denote the minimalpolynomial of η and $\eta^2 - 11\eta - 1$, respectively, and put $h(z) = z^2 - 11z - 1$. Then $q(z)$ divides the resultant

$$q_1(z) = Res_y(z - h(y), P(y))$$

by Theorem 8 in [2]. A simple computation using MAPLE V results

$$\begin{aligned} q_1(z) &= z^3 - (v^2 - 11v - 2m_1 - 3)z^2 \\ &\quad -(2v^2 - 24v + 11vm_1 - m_1^2 - 125m_1 + 30)z \\ &\quad -v^2 + 134v - 11vm_1 + m_1^2 + 112m_1 - 1364. \end{aligned}$$

Since the constant term of $q_1(z)$ is $\varepsilon_1 5^n$ we obtain the following quadratic equation for the integer m_1 :

$$m_1^2 - m_1(11v - 112) - v^2 + 134v - 1364 - \varepsilon_1 5^n = 0.$$

The discriminant of this equation in m_1 has to be a square of an integer w; thus , after a simple computation, we obtain

$$w^2 - 125(-v + 12)^2 = -4\varepsilon_1 \cdot 5^n = \pm 4 \cdot 5^n, \tag{2}$$

$$m_1 = \frac{11v - 112 + w}{2}. \tag{3}$$

Equation (2) is obviously unsolvable for $n = 1$, hence our assertion in true in this case. Now we distinguish three cases.

Case 1. Let $n = 2(k + 1)$ with a $k \in \mathbb{Z}_{\geq 0}$ and suppose that $v, w \in \mathbb{Z}$ form a solution of (2). We claim that there exists an $m \in \mathbb{Z}_{\geq 0}$ such that $w = \varepsilon_4 \cdot 5^{k+1} L_m$ and $-v + 12 = \varepsilon_2 \cdot 5^k \cdot F_m$ with $\varepsilon_2, \varepsilon_4 \in \{1, -1\}$ and $k \in \mathbb{Z}_{\geq 0}$. The assertion of Lemma 1 then follows immediately.

Of course, this claim is true for $k = 0$ for we then have $w = 5w_1$ with an $w_1 \in \mathbb{Z}$ and after division by 25 equation (2) becomes

$$w_1^2 - 5(-v + 12)^2 = \pm 4.$$

We can now apply $(P1)$ to get the asserted expressions for v and w.

Suppose now that the claim is true for a $k \geq 0$. Then, as

$$w^2 - 125(-v + 12)^2 = \pm 4 \cdot 5^{2(k+2)}$$

we have $w = 5w_1$ with a $w_1 \in \mathbb{Z}$ and $5|(-v + 12)$. Thus

$$w_1^2 - 125\left(\frac{-v + 12}{5}\right)^2 = \pm 4 \cdot 5^{2(k+1)}.$$

The claim follows by induction.

Inserting the values of v and w into (3) we obtain

$$m_1 = \frac{11(12 - \varepsilon_2 \cdot 5^k F_m) - 112 + \varepsilon_4 \cdot 5^{k+1} L_m}{-2} = 10 + 5^k \frac{-11\varepsilon_2 F_m + 5\varepsilon_4 L_m}{2}.$$

We have $F_5 = F_{-5} = 5$ and $-L_5 = L_{-5} = -11$ by $(P2)$, hence by $(P3)$

$$m_1 = \begin{cases} 10 + 5^k \varepsilon_2 L_{m-5} & \text{, if } \varepsilon_2 = \varepsilon_4 \\ 10 - 5^k \varepsilon_2 F_{m+5} & \text{, if } \varepsilon_2 = -\varepsilon_4, \end{cases}$$

which can be summarized in the form $m_1 = 10 + 5^k \varepsilon_2 \varepsilon_3 F_{m-5\varepsilon_3}$. This proves Lemma 1 in Case 1.

Case 2. Let $n = 2(k+1)+1$ with a $k \in \mathbb{Z}_{\geq 0}$. This case can be treated analogously to Case 1. One needs only observe that, for odd n's the role of w and $-v+12$ is to be interchanged. Furthermore in the final step, one has to use $(P4)$ instead of $(P3)$.

Case 3. Let $n = 0$. Then (2) becomes

$$w^2 - 5(5(-v+12))^2 = \pm 4.$$

Hence, by $(P1)$, $w = \varepsilon_3 L_{m'}$ and $5(-v+12) = \varepsilon_2 \cdot F_{m'}$ for some $m' \in \mathbb{Z}_{\geq 0}$ and $\varepsilon_2, \varepsilon_3 \in \{1, -1\}$. By $(P7)$, we know that $5|m'$ and hence, on putting $m' = 5m$ the relations

$$-v = -12 + \varepsilon_2 \cdot 5^k F_{5m} \text{ and } w = \varepsilon_3 L_{5m}$$

hold with $k = -1$. Now m_1 can be transformed into the asserted form as in Case 1.□

In the sequel, $\left(\frac{x}{m}\right)$ will denote the Jacobi symbol for coprime integers x, m. The following two lemmata play a crucial role in the proof of the Theorem. They are generalizations of Lemmata 2 and 3 in [2].

Lemma 2 *Fix an integer h, a polynomial $H(x,y) \in \mathbb{Z}[x,y]$, a set $\mathcal{P} = \{p_1, \ldots, p_t\}$ of a primes and let $\{G_m\}$ be one of the sequences defined in Lemma 1. Let $r(p)$ denote the minimal period of the sequence $\{G_m \bmod p\}$ for $p \in \mathcal{P}$, put $lcm[r(p_1), \ldots, r(p_t)] = R$ and choose $\mathcal{M} = \{m_1, \ldots, m_s\}$ as a set of integers satisfying $0 \leq m_1 < m_2 < \ldots < m_s < R$. If, for each $m \in \mathcal{M}$ there exists a $p \in \mathcal{P}$ such that*

$$\left(\frac{H(G_m, G_{m+h})}{p}\right) = -1 \tag{4}$$

then any solution $x, z \in \mathbb{Z}$ of the diophantine equation

$$H(G_x, G_{x+h}) = z^2 \tag{5}$$

satisfies the incongruences $x \not\equiv m_i \pmod R$ $1 \leq i \leq s$.

Before giving the proof, we formulate a simple consequence of Lemma 2, which is very useful with respect to proofs of unsolvability of diophantine equations of form (5).

Corollary *Let the notation be the same as in Lemma 2. If for each* $0 \leq m < R$ *there exists a* $p \in \mathcal{P}$ *such that (4) holds, then (5) has no solution* $x, z \in \mathbb{Z}$.

Proof of Lemma 2. Suppose that $x, z \in \mathbb{Z}$ is a solution of (5) such that $x \bmod R \in \mathcal{M}$. We may assume without loss of generality that $x \equiv m_1 \pmod R$. For $x, z \in \mathbb{Z}$ to be a solution of (5), it is necessery that

$$\left(\frac{H(G_x, G_{x+h})}{p}\right) = 1$$

for any prime number p.

On the other hand by the hypothesis there exists a prime $p \in \mathcal{P}$ such that

$$\left(\frac{H(G_{m_1}, G_{m_1+h})}{p}\right) = -1.$$

As $x \equiv m_1 \bmod R$ and $r(p)|R$ we have a fortiori $x \equiv m_1 \pmod{r(p)}$, thus $G_x \equiv G_{m_1} \pmod p$ and $G_{x+h} \equiv G_{m_1+h} \pmod p$. Hence

$$H(G_x, G_{x+h}) \equiv H(G_{m_1}, G_{m_1+h}) \pmod p;$$

thus the last two equations are contradictory. This proves Lemma 2. □

A typical application of Lemma 2 is to prove, with an appropriate choice of the set of $\mathcal{P}$, that all solutions of (5) in x belong to some residue classes mod R. Enlarging the set $\mathcal{P}$ we can prove the same result with respect to an $R' > R$. But this process does not yield a complete solution of (5), for when $x_0 \in \mathbb{Z}$ is a solution of (5), then $H(G_x, G_{x+h})$ is a quadratic residue mod R for all x belonging to the residue class x_0 mod R. The next lemma serves the purpose of showing that, in a fixed residue class with respect to a sufficiently large modulus R, at most one integer x can be part of a solution of (5). The lemma at the same time also provides a method for constructing the modulus R.

Lemma 3 *Let* $H(x, y) \in \mathbb{Z}[x, y], m_0, h \in \mathbb{Z}$ *and* $\mathcal{P} = \{p_1, \ldots, p_t\}$ *a set of primes with* $p_i \geq 5, 1 \leq i \leq t$. *Suppose that there exist* $a, b_1, \ldots, b_t \in \mathbb{Z}_{>0}$ *such that, for any* $\alpha \geq a - 1$ *there exist integers* $\beta_1, \ldots, \beta_t$ *with* $0 \leq \beta_i \leq b_i$ $(i = 1, \ldots, t)$ *for which*

$$\left(\frac{H(-G_{m_0}, -G_{m_0+h})}{L_{2^\alpha p_1^{\beta_1} \cdots p_t^{\beta_t}}}\right) = -1 \tag{6}$$

hold. Then equation (5) has at most one solution $x, z \in \mathbb{Z}$ *satisfying*

$$x \equiv m_0 \ (mod\ 2^{a+1} p_1^{b_1} \cdots p_t^{b_t}),$$

namely $x = m_0$.

Proof. Let $x, z \in \mathbb{Z}$ be a solution of (5) with $x = m_0 + 2^{a+1}p_1^{b_1}\cdots p_t^{b_t}\cdot n$ for $0 \neq n \in \mathbb{Z}$. Write $n = \pm 2^c \cdot 3^d n_1$ with n_1 odd and $3 \not| n_1$. Then we have $L_{2^{a+c-1}p_1^{b_1}\cdots p_t^{b_t}} | L_{2^{a+c-1}p_1^{b_1}\cdots p_t^{b_t}\cdot n_1}$ by $(P8)$ and by $(P5)$ it then follows that

$$G_x \equiv -G_{m_0} \pmod{L_{2^{a+c-1}p_1^{b_1}\cdots p_t^{b_t}}}$$

and

$$G_{x+h} \equiv -G_{m_0+h} \pmod{L_{2^{a+c-1}p_1^{b_1}\cdots p_t^{b_t}}}.$$

Therefore,

$$H(G_x, G_{x+h}) \equiv H(-G_{m_0}, -G_{m_0+h}) \pmod{L_{2^{a+c-1}p_1^{b_1}\cdots p_t^{b_t}}}. \tag{7}$$

Choose $\alpha = a + c - 1 \geq a - 1$. Then, by hypothesis (6) holds for some $(\alpha, \beta_1, \ldots, \beta_t)$ with $0 \leq \beta_i \leq b_i,\ 1 \leq i \leq t$. By $(P8)$, we know that $L_{2^\alpha p_1^{\beta_1}\cdots p_t^{\beta_t}} | L_{2^\alpha p_1^{b_1}\cdots p_t^{b_t}}$ and then (7) yields

$$H(G_x, G_{x+h}) \equiv H(-G_{m_0}, -G_{m_0+h}) \pmod{L_{2^\alpha p_1^{\beta_1}\cdots p_t^{\beta_t}}}.$$

This congruence together with (6) contradicts the hypothesis that $x, z \in \mathbb{Z}$ form a solution of (5). The lemma is proved. □

3 Proof of the Theorem

At this stage we have at hand most of the auxiliary results which we need in order to prove our Theorem. We shall see that it is a direct consequence of the following proposition

Proposition 1 *Let*

$$\begin{aligned} D(u,w) &= 15125 + 1464w - 3948u - 462uw + 24w^2 \\ &\quad -24uw^2 + 244u^2 + 20u^2w + u^2w^2 - 4u^3 - 4w^3 \end{aligned}$$

and $\{G_m\}_{-\infty}^{\infty}$ *one of the sequences defined in Lemma 1. Then the diophantine equation*

$$D(\varepsilon_2 5^k G_m, \varepsilon_2\varepsilon_3 5^k G_{m-5\varepsilon_3}) = y^2 \tag{8}$$

has only the following solutions in non-negative integers k, m, y *and* $\varepsilon_2, \varepsilon_3 \in \{-1, 1\}$

F_m :	$(k, m, y, \varepsilon_2, \varepsilon_3)$	$(1, 0, 65, 1, 1)$	$(1, 4, 4075, 1, -1)$	$(0, 3, 163, -1, 1)$
L_m :		$(1, 1, 520, -1, 1)$	$(0, 2, 63, 1, 1)$	$(1, 2, 65, 1, 1)$
$F_{5m}/5$:		$(-1, 0, 117, 1, -1)$	$(-1, 5, 139, -1, 1)$.	

Before proving the Proposition we shall show how it implies the Theorem.

Proof of the Theorem. Let η be a solution of (1) with $\varepsilon = -1$. Then $-1/\eta$ solves (1) with $\varepsilon = 1$, thus, in the sequel, we may assume $\varepsilon = -1$. Then by Lemma 1, η is a zero of $P(z; k, m, \varepsilon_2, \varepsilon_3)$ for some values of the parameters $k, m, \varepsilon_2, \varepsilon_3$. It is well known that the discriminant of a defining polynomial of a cyclic cubic number field is a square of an integer.

Let

$$p(z; u, w) = z^3 + (-12 + u)z^2 + (10 + w)z + 1$$

so that we have

$$p(z; \varepsilon_2 5^k G_m, \varepsilon_2 \varepsilon_3 5^k G_{m-5\varepsilon_3}) = P(z; k, m, \varepsilon_2, \varepsilon_3).$$

A simple computation shows that the discriminant of $p(z; u, w)$ is $D(u, w)$. Thus to determine all cyclic cubic number fields which contain an element η satisfying (1), it is enough, by Lemma 1, to solve (8) for the recursive sequences $G_m = F_m, L_m$ and $F_{5m}/5$.

The solutions of (8) given in the Proposition yield the number fields 2.,3. and 5. for the Fibonacci sequence; the fields 4.,7. and 8., for the Lucas sequence and finally the fields 1. and 6. for $F_{5m}/5$. The Theorem is proved. □

4 Proof of the Proposition

We first require a lemma.

Lemma 4 *Equation (8) has no solution for $k \geq 2, m \geq 0$.*

Proof. Let $k \geq 3, m \geq 0$ and $\varepsilon_2, \varepsilon_3 \in \{-1, 1\}$ be fixed. Then $D = D(\varepsilon_2 5^k G_m, \varepsilon_2 \varepsilon_3 5^k G_{m-5\varepsilon_3})$ is an integer. We shall prove that $5^4 | (D - 15125)$. As $5^3 \| 15125$ this implies that $5^3 \| D$ and D can not be a square of an integer. In fact this claim is trivially true for $k \geq 4$. Define $A = 1464\varepsilon_3 G_{m-5\varepsilon_3} - 3948 G_m$. For $k = 3$ we have $5^6 | (D - \varepsilon_2 \cdot 5^k A - 15125)$ and we want to prove that $5 | A$.

We obviously have

$$A \equiv 4\varepsilon_3 G_{m-5\varepsilon_3} + 2G_m \pmod 5.$$

It is easy to see that $G_{m+5} = 8G_m + 5G_{m-1}$ for any $m \in \mathbb{Z}$, which implies that

$$A \equiv \begin{cases} -32G_m + 2G_m, & \text{if } \varepsilon_3 = -1 \\ 4G_{m-5} + 16G_{m-5}, & \text{if } \varepsilon_3 = 1 \end{cases} \pmod 5$$

Thus $A \equiv 0 \pmod 5$ in both cases. Therefore equation (8) is not solvable for $k \geq 3$.

Now we consider the case $k = 2$ and suppose that n is odd. Then by Lemma 1 $G_m = L_m$. Since the relation $5 | A$ holds also for $k \leq 2$, we have $5^3 | D$. Assume

that (8) is solvable then we must even have $5^4|D$ since D is a square. We shall prove that this is impossible. In fact if $5^4|D$, then

$$D \equiv 15125 + \varepsilon_2 5^k (1464\varepsilon_3 L_{m-5\varepsilon_3} - 3948 L_m) \equiv 0 \pmod{5^4}.$$

On dividing by 25, we see that the quantity $D_1 := D/5^3$ satisfies

$$5D_1 \equiv 5 + \varepsilon_2(14\varepsilon_3 L_{m-5\varepsilon_3} + 2L_m) \equiv 0 \pmod{25}.$$

By virtue of the identity $L_{m+5} = 8L_m + 5L_{m-1}$ we obtain

$$5D_1 \equiv \begin{cases} 5(1 - 2\varepsilon_2(L_m + 2L_{m-1})), & \text{if } \varepsilon_3 = -1 \\ 5(1 + \varepsilon_2(L_{m-5} + 2L_{m-6})), & \text{if } \varepsilon_3 = 1 \end{cases} \pmod{25}.$$

But it is easy to check that $L_m + 2L_{m-1} \equiv 0 \pmod 5$ holds for any $m \in \mathbb{Z}$, hence $D_1 \equiv 1 \bmod 5$ in contradiction to $5^4|D$.

In the remaining case, when $k = 2$ and n is even, the solvability of equation (8) cannot be disproved in the same way. This can be seen as follows: We have $G_m = F_m$ and by the same computation obtain the condition

$$0 \equiv D_1 \equiv \begin{cases} 1 - 2\varepsilon_2(F_m + 2F_{m-1}), & \text{if } \varepsilon_3 = -1 \\ 1 + \varepsilon_2(F_{m-5} + 2F_{m-6}), & \text{if } \varepsilon_3 = 1 \end{cases} \pmod 5.$$

Since it is easy to show that $F_m + 2F_{m-1} \equiv L_m \pmod 5$ for any $m \in \mathbb{Z}$ we see that $D_1 \equiv 0 \pmod 5$ holds for any choice of ε_2 and ε_3.

Therefore we use an other argument. We invoke the corollary of Lemma 2 choosing $H(x, y; \varepsilon_2, \varepsilon_3) = D(\varepsilon_2 \cdot 5^2 x, \varepsilon_2\varepsilon_3 5^2 y), h = -5\varepsilon_3$ and the set of primes $\mathcal{P} = \mathcal{P}_1 = \{3, 11, 17, 19, 31, 41, 61\ , 107, 181, 541, 2521\}$. Then one easily checks that $r(p)|360$ for any $p \in \mathcal{P}_1$. We compute

$$J(m, p; \varepsilon_2, \varepsilon_3) = \left(\frac{H(F_m, F_{m+h})}{p}\right)$$

for each $0 \le m < 360$ and each $p \in \mathcal{P}_1$ and found a $p = p(m, \varepsilon_2, \varepsilon_3) \in \mathcal{P}_1$ with $J(m, p; \varepsilon_2, \varepsilon_3) = -1$ for each possible choice of $\varepsilon_2, \varepsilon_3 \in \{-1, 1\}$ and each $0 \le m < 360$. Hence, by the Corollary, (8) is not solvable for $k = 2$ and n even, and so Lemma 4 is completely proved.□

Proof of the Proposition. By Lemma 4, we need to consider equation (8) only for $k = -1, 0, 1$. The proof, carried out essentially by means a computer, is divided into three steps.

Step 1. Exclusion of those triples $(k, \varepsilon_2, \varepsilon_3)$ for which (8) is unsolvable and computation of the small solutions m_0 of (8) in the case of solvability was achived by means of Lemma 2.

Step 2. This is a search for a small set of primes which enables us to exclude solutions of (8) by means of Lemma 3.

Step 3. Using Lemma 2 we prove that if, for some triple $(k, \varepsilon_2, \varepsilon_3)$, m is a solution of (8), then

$$m \equiv m_0 \pmod{2^{a+1} p_1^{b_1} \dots p_t^{b_t}}$$

for some suitable primes $p_1, \dots, p_t$ and integers $a, b_1, \dots, b_t$. In what follows we specify the parameters used in each step and the results of the computations.

In Step 1 we tested (8) for any possible choice of the parameters $(\varepsilon_2, \varepsilon_3, n, k)$ using Lemma 2 with the set of primes $\mathcal{P}_2 = \mathcal{P}_1 \cup \{5, 7, 23, 241, 2161\}$. We have $r(p) | 720$ for any $p \in \mathcal{P}_2$. In Table 1 we exhibit the result of the test. A number m_0 in the table indicates that, if m is a solution of (8), then $m \equiv m_0 \pmod{720}$, while an asterisk * indicates that, for that choice of parameters, (8) is not solvable.

(n,k)	(5,1)	(3,0)	(4,1)	(2,0)	(0,-1)
$(\varepsilon_2, \varepsilon_3)$					
(1,1)	2	2	0	*	*
(1,-1)	718,719	718	4	*	0
(-1,-1)	*	*	0	717	719
(-1,1)	1	*	716	3	0,1

Table 1.

Using (**P2**) it is easy to check that

$$P(z; k, -m, \varepsilon_2, \varepsilon_3) = \begin{cases} P(z; k, m, \varepsilon_2, -\varepsilon_3), & \text{if } m+n \text{ is odd} \\ P(z; k, m, -\varepsilon_2, -\varepsilon_3), & \text{if } m+n \text{ is even.} \end{cases}$$

Hence, by Table 1, it is enough to consider the following values: $(n, k, \varepsilon_2, \varepsilon_3) = (5,1,1,1), (5,1,-1,1), (3,0,1,1), (4,1,1,1), (4,1,1,-1), (2,0,-1,1), (0,-1,1,-1), (0,-1,-1,1)$. Let $m_0 = m_0(n, k, \varepsilon_2, \varepsilon_3)$ denote the value shown at the corresponding place in Table 1. Let

$$H(x, y) = H(x, y; k, \varepsilon_2, \varepsilon_3) = D(\varepsilon_2 5^k x, \varepsilon_2 \varepsilon_3 5^k y).$$

In Step 2 we search for suitable sets $\mathcal{P}$ of primes for which we can apply Lemma 3 with suitable exponents $a, b_1, \dots, b_t$. In Table 2 we summarize the result of this search. In the column D_{m_0} we list the value of $D(-G_{m_0}, -G_{m_0 - 5\varepsilon_3})$ and in the rows columnwise headed by the primes $2, p_1 = 5, \dots, p_7 = 37$ we display the respective exponents $a, b_1, \dots, b_t$ for which we were able to verify the hypothesis of Lemma 3. Here a hyphen indicates here that the coresponding prime did not enter into the calculation.

$(n,k,\varepsilon_2,\varepsilon_3)$	m_0	D_{m_0}	2	5	7	11	13	17	31	37
(5,1,1,1)	2	$3^3\cdot 5^2\cdot 907$	4	2	2	1	-	-	-	-
(5,1,-1,1)	1	$-2^5\cdot 5^2\cdot 337$	3	2	1	-	1	-	-	-
(3,0,1,1)	2	$47\cdot 911$	5	2	-	-	-	-	-	-
(4,1,1,1)	0	$3^3\cdot 5^2\cdot 83$	4	2	-	-	-	-	-	-
(2,0,-1,1)	3	7537	3	2	1	1	-	1	1	1
(4,1,1,-1)	4	$3^3\cdot 5^2\cdot 419$	4	2	1	-	1	-	-	-
(0,-1,1,-1)	0	$17\cdot 977$	3	1	2	1	-	-	-	-
(0,-1,-1,1)	1	$7^2\cdot 233$	3	1	2	-	-	-	-	-

Table 2.

In Step 3 we prove that, if $m = m(n,k,\varepsilon_2,\varepsilon_3)$ solves (8), then

$$m \equiv m_0 \pmod{2^a\cdot 5^{b_1}\cdot 7^{b_2}\cdot 11^{b_3}\cdot 13^{b_4}\cdot 17^{b_5}\cdot 31^{b_6}\cdot 37^{b_7}} \tag{9}$$

for the numbers $a, b_1, \ldots, b_7$ listed in the row $(n,k,\varepsilon_2,\varepsilon_3)$ of Table 2. Indeed, if we are able to verify (9), then, by Lemma 3, we conclude that $m = m_0$.

For this purpose we once again apply Lemma 2, this time for the following eight sets of primes corresponding to the eight cases of Table 2. The associated values of R are also listed.

$$\begin{aligned}
\mathcal{P}_3 &= \{3,7,11,13,29,41,71,97,101,151,281,401,491,701,911,1471,2161,2801,3001\},\\
R &= 16900 = 2^4\cdot 5^2\cdot 7^2\\
\mathcal{P}_4 &= \{13,17,19,29,83,97,107,167,211,281,293,421,503,587,1009,1427,3527,3529\},\\
R &= = 2^4\cdot 3^2\cdot 7^2\\
\mathcal{P}_5 &= \{3,7,23,47,127,383,769,1087,1103,2207,3167\},\\
R &= = 2^8\cdot 3\\
\mathcal{P}_6 &= \{43,89,197,199,263,307,331,661,881,967,991,1321,2179,2731,3169\},\\
R &= 7920 = 2^4\cdot 3^2\cdot 11\cdot 5\\
\mathcal{P}_7 &= \{79,103,131,233,467,521,859,1171,1249,1637,1951,2081,2341,2731,3121\},\\
R &= 2^4\cdot 3^2\cdot 5\cdot 13 = 9360\\
\mathcal{P}_8 &= \{3,7,11,23,31,41,61,67,409,919,1021\},\\
R &= 4080 = 2^4\cdot 3\cdot 5\cdot 17\\
\mathcal{P}_9 &= \{3,7,11,23,31,41,61,557,743,2417,311,1489,1861,2791,3347\},\\
R &= 22320 = 2^4\cdot 3^2\cdot 5\cdot 31\\
\mathcal{P}_{10} &= \{3,7,11,23,31,41,61,73,149,443,887,2663,1481,3331,2221\},\\
R &= 8880 = 2^4\cdot 3\cdot 5\cdot 37.
\end{aligned}$$

On employing this sets of primes one verifies that Table 2 contains all solutions of equation (8). This proves the Proposition. □

References

[1] [1] J.H.E. Cohn, *On square Fibonacci numbers,* J. London Math. Soc. **39** (1964), 537-540.

[2] I. Gaál, A. Pethő and M. Pohst, *On the resolution of index form equations in dihedral quartic number fields,* Experimental Math. **3** (1994), 245–254.

[3] G.W. Fung, H. Ströher, H.C. Williams and H.G. Zimmer, *Torsion groups of elliptic curves with integral j-invariant over pure cubic number fields,* J. NUmber Theory **36** (1990), 12–45.

[4] R. Loos, *Computing in algebraic extensions,* in: Computer Algebra Symbolic and Algebraic Computation, Eds.: B. Buchberger, G.E. Collins and R. Loos in cooperation with R. Albrecht, Springer Verlag 1983, pp. 173–187.

[5] A. Pethő, *Full cubes in the Fibonacci sequences,* Publ. Math. Debrecen **30** (1983), 117-127.

[6] A. Pethő, *Application of Gröbner basis to the resolution of systems of norm equations,* in Proc. ISSAC'91, ed.: S. M. Watt, ACM Press, 1991. pp. 144-150.

[7] A. Pethő, Th.Weis and H.G. Zimmer, *Torsion groups of elliptic curves with integral j-invariant over general cubic number fields,*, J. Algebra and Comp. to appear

[8] P. Ribenboim, *Square classes of Fibonacci and Lucas numbers,* Portugaliae Math. **46** (1989), 159-175.