ACTA ARITHMETICA
127.2 (2007)

# On the equation $x^2 + dy^2 = F_n$

by

CHRISTIAN BALLOT (Caen) and FLORIAN LUCA (Morelia)

**1. Introduction.** Let $(F_n)_{n\geq 0}$ be the Fibonacci sequence given by $F_0 = 0$, $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$. Let $d$ be any fixed rational integer. Using standard sieve methods it is easy to establish that, for $\sqrt{-d}$ not an integer, most positive integers $m$ are not representable as $m = |x^2 + dy^2|$ with $x$ and $y$ integers. In this paper, we look at those positive integers $m$ which are both members of the Fibonacci sequence and are representable as $|x^2 + dy^2|$ for some integers $x$ and $y$. That is, we investigate the set

$$\mathcal{N}_d = \{n > 0 : F_n = |x^2 + dy^2| \text{ for some integers } x \text{ and } y\}. \tag{1}$$

Clearly, $\mathcal{N}_0$ consists of the positive integers $n$ such that $F_n$ is a perfect square and Cohn [1] showed that $\mathcal{N}_0 = \{1, 2, 12\}$. When $d = 1$, using the formula

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

we see that $\mathcal{N}_1$ contains all odd positive integers. Furthermore, since $F_n$ and $F_{n+1}$ are coprime, every odd prime factor of $F_{2n+1}$ is congruent to 1 modulo 4. In [2], it was shown that for most even positive integers $n$, $F_n$ admits a prime factor $q \equiv 3 \pmod 4$. Here, we go one step further. In order to settle the case of $\mathcal{N}_1$, we first prove the following result.

PROPOSITION 1. *For all even positive integers $n$ except a set of asymptotic density zero, there exists a prime $q \equiv 3 \pmod 4$ such that $q \mid F_n$ and the exact power of $q$ that divides $F_n$ is odd.*

Since for $q \equiv 3 \pmod 4$, $-1$ is a quadratic nonresidue $\pmod q$, Proposition 1 immediately implies that the asymptotic density of $\mathcal{N}_1$ is precisely $1/2$.

Note also that if $d$ is a perfect square, then $\mathcal{N}_d$ has positive lower asymptotic density. Indeed, if we write $\varrho(d)$ for the rank of appearance of $d$ in $(F_n)_{n\geq 0}$, i.e., $\varrho(d)$ is the minimal positive integer $k$ such that $d \mid F_k$, then formula (2) implies that if $d$ is a perfect square, then the set $\mathcal{N}_d$ contains

2000 *Mathematics Subject Classification*: 11B39, 11N37.

 

the set

$$\{2n+1 : n \equiv 0, -1 \pmod{\varrho(d)}\},$$

which is of positive asymptotic density. But $\mathcal{N}_d$ also has positive lower asymptotic density if $d$ is the opposite of a perfect square. Indeed, $\mathcal{N}_d$ then contains

$$\{n : \varrho(4d) \mid n\}.$$

If we put $d = -t^2$, then $F_n/t^2$ is an integer multiple of 4 for $n$ divisible by $\varrho(4d)$. As such, $F_n/t^2$ can be written as $(x-y)(x+y)$. Hence $F_n = (tx)^2 - (ty)^2 = (tx)^2 + dy^2$. Therefore we have shown the following result.

Theorem 2. *For any $d$ which is plus or minus a perfect square, the set $\mathcal{N}_d$ has positive lower asymptotic density. The asymptotic density of $\mathcal{N}_1$ is* $1/2$.

We put

$$\mathcal{D} = \{d \in \mathbb{Z} : \mathcal{N}_d \text{ has positive lower asymptotic density}\}.$$

Theorem 2 implies that $\mathcal{D}$ is an infinite set. However, in this paper, we show that most integers do not belong to $\mathcal{D}$. For a positive real number $x$ we write $\mathcal{D}(x)$ for the set of $d \in \mathcal{D}$ with $|d| \le x$.

Theorem 3. *There exists a positive constant $C$ such that if $x > 1$ is any real number then*

$$\#\mathcal{D}(x) \le C\,\frac{x}{(\log x)^3}.$$

By a standard procedure of partial summation, Theorem 3 implies that

$$\sum_{d \in \mathcal{D}} \frac{1}{|d|} < \infty$$

(note that $0 \notin \mathcal{D}$).

We would like to make the following conjecture.

Conjecture 4. *$\mathcal{D}$ contains only finitely many integers not a square or the negative of a square.*

For integers $a$ and $b$ with $b > 0$ odd, we write $\left(\frac{a}{b}\right)$ for the Jacobi symbol of $a$ with respect to $b$. We state another related conjecture.

Conjecture 5. *For all but finitely many of the integers $d$ not a square or the negative of a square, there is a prime $q \ge 5$ such that*

$$\left(\frac{d}{F_q}\right) = -1.$$

The argument used in the proof of Lemma 9 below shows that Conjecture 5 implies Conjecture 4. If true, Conjecture 4 would imply a stronger bound on the cardinality of $\mathcal{D}(x)$ than the one provided by Theorem 3. We would like to leave these conjectures as problems to the reader. In fact, it may be that Conjecture 5 is true without exceptions.

Throughout this paper, we assume familiarity with basic properties of Fibonacci and Lucas numbers. The $n$th Lucas number is denoted by $L_n$. We recall here that for a prime $p$, the rank of appearance $\varrho(p)$ of $p$ in the Fibonacci sequence divides $p - e_p$, where $e_p$ is the Legendre symbol of 5 with respect to $p$. Also, we use the Vinogradov symbols $\gg$ and $\ll$ and the Landau symbols $O$ and $o$ with their regular meanings. The constants implied in them are absolute. For a positive real number $x$, we use $\log x$ for the maximum between the natural logarithm of $x$ and 1. We write $\pi(x)$ for the number of primes $p \le x$, and for coprime integers $1 \le a \le b$ we write $\pi(x; a, b)$ for the number of primes $p \le x$ congruent to $a$ modulo $b$. We use $p$, $q$ and $r$ to denote prime numbers. For a set $\mathcal{A}$ of positive integers we put $\mathcal{A}(x) = \mathcal{A} \cap [1, x]$.

**Acknowledgements.** This paper was written in part during a very enjoyable visit by the second author to the Laboratoire Nicolas Oresme of the University of Caen; he wishes to express his thanks to that institution for the hospitality and support. During the preparation of this paper, F. L. was also partly supported by grants SEP-CONACYT 46755, PAPIIT IN104505 and a Guggenheim Fellowship.

**2. The proofs.** For any positive integer $n$ we let $P(n)$ denote the largest prime factor of $n$, and for real numbers $x \ge y \ge 1$ we put $\Psi(x, y) = \{n \le x : P(n) \le y\}$. The numbers belonging to $\Psi(x, y)$ are usually referred to as *smooth numbers*. The following estimate for the number of smooth numbers (see Section III.5.4 of Tenenbaum's book [3]) will play a crucial rôle in our proofs.

LEMMA 6. *Let $\varepsilon > 0$ be fixed. Uniformly for*

$$\exp((\log\log x)^{5/3+\varepsilon}) \le y \le x$$

*we have*

$$\#\Psi(x, y) = x \exp(-(1 + o(1))u \log u), \quad \textit{where} \quad u = \frac{\log x}{\log y}.$$

Let $1 \le a \le b$ be fixed coprime integers. For a positive real number $x$ we put

$$\mathcal{A}(x; a, b) = \{n \le x : \text{if } p \mid n \text{ and } p > \log x, \text{ then } p \not\equiv a \pmod{b}\},$$

that is, $n$ is in $\mathcal{A}(x; a, b)$ if no prime factor of $n$ larger than $\log x$ is congruent to $a \pmod{b}$.

We will need the following estimate.

LEMMA 7. *If* $1 \le a \le b$ *are coprime, then there exists* $x_{a,b}$ *such that*

$$\#\mathcal{A}(x;a,b) \ll \frac{x(\log\log x)^2}{(\log x)^{1/\phi(b)}} \quad \text{for } x > x_{a,b}.$$

*Proof.* Let $x$ be a large real number and let $y=x^{1/\log\log x}$, $u=\log x/\log y = \log\log x$. We put $\mathcal{A}_1(x) = \mathcal{A}(x;a,b) \cap \Psi(x,y)$. Then, by Lemma 6,

$$\#\mathcal{A}_1(x) \le \#\Psi(x,y) = x\exp(-u(1+o(1))\log u) < \frac{x}{\log x} \tag{3}$$

for large $x$. We now put $\mathcal{A}_2(x) = \mathcal{A}(x;a,b) \setminus \mathcal{A}_1(x)$. To bound $\#\mathcal{A}_2(x)$, let $n \in \mathcal{A}_2(x)$ and write $n = Pm$, where $P = P(n) > y$. Then $m < x/y$. Thus, fixing $m$, we see that the number of choices for $P$ is

$$\le \pi(x/m) \ll \frac{x}{m\log(x/m)} \ll \frac{x}{m\log y} = \frac{x\log\log x}{m\log x}.$$

Note that $m \le x$ is an integer which is free of primes $p \equiv a \pmod b$ larger than $\log x$. Write $\mathcal{M}(x)$ for the set of such positive integers $m$. Then, summing up over all possible choices of $m \in \mathcal{M}(x)$, we get

$$\begin{aligned}
\#\mathcal{A}_2(x) &\ll \frac{x\log\log x}{\log x}\sum_{m\in\mathcal{M}(x)}\frac{1}{m} \\
&\le \frac{x\log\log x}{\log x}\prod_{\substack{p\le x\\ p\not\equiv a \,(\mathrm{mod}\, b)}}\Big(\sum_{\alpha\ge 0}\frac{1}{p^\alpha}\Big)\prod_{\substack{p\le \log x\\ p\equiv a \,(\mathrm{mod}\, b)}}\Big(\sum_{\alpha\ge 0}\frac{1}{p^\alpha}\Big) \\
&= \frac{x\log\log x}{\log x}\prod_{\substack{p\le x\\ p\not\equiv a \,(\mathrm{mod}\, b)}}\Big(1-\frac{1}{p}\Big)^{-1}\prod_{\substack{p\le \log x\\ p\equiv a \,(\mathrm{mod}\, b)}}\Big(1-\frac{1}{p}\Big)^{-1} \\
&= \frac{x\log\log x}{\log x}\exp\Big(\sum_{\substack{p\le x\\ p\not\equiv a \,(\mathrm{mod}\, b)}}\frac{1}{p}+\sum_{\substack{p\le \log x\\ p\equiv a \,(\mathrm{mod}\, b)}}\frac{1}{p}+O(1)\Big) \\
&= \frac{x\log\log x}{\log x}\exp\Big(\frac{\phi(b)-1}{\phi(b)}\log\log x+\frac{1}{\phi(b)}\log\log\log x+O(1)\Big) \\
&\ll \frac{x(\log\log x)^2}{(\log x)^{1/\phi(b)}},
\end{aligned} \tag{4}$$

where we used the fact that for any fixed $A > 0$, the estimate

$$\sum_{\substack{p\le y\\ p\equiv c \,(\mathrm{mod}\, b)}}\frac{1}{p} = \frac{\log\log y}{\phi(b)} + O\Big(\frac{\log b}{b}\Big) \tag{5}$$

holds uniformly in the range $y \ge 3$ and $1 \le c \le b < (\log y)^A$ with $c$ and $b$

coprime. In particular, the above estimate also holds when $b$ is fixed. This completes the proof of the lemma. ■

We will also need the following lemma.

LEMMA 8. *Let $\mathcal{B}(x)$ be the set of integers $n \le x$ divisible by a product of primes $pq$, where $p > \log x$ and $q \equiv \pm 1 \pmod p$. Then*

$$\#\mathcal{B}(x) \ll \frac{x \log\log x}{\log x}.$$

*Proof.* Let $x$ be large and fix two primes $p$ and $q$ such that $p > \log x$, $q \equiv \pm 1 \pmod p$ and $pq < x$. The number of positive integers $n \le x$ such that $pq \mid n$ is $\le x/pq$. Summing up over all possible choices of $p$ and $q$, we get

$$\#\mathcal{B}(x) \le x \sum_{\log x < p \le x} \sum_{\substack{q \le x \\ q \equiv \pm 1 \pmod p}} \frac{1}{pq} = x(S_1 + S_2), \tag{6}$$

where $S_1$ is the contribution to the double sum from primes $p < (\log x)^3$, and $S_2$ is the contribution from primes $p \ge (\log x)^3$. Let

$$T_p = \sum_{\substack{q \le x \\ q \equiv \pm 1 \pmod p}} \frac{1}{pq}.$$

Using estimate (5) with $A = 3$ when $p < (\log x)^3$, we get

$$T_p \ll \frac{\log\log x}{p^2}.$$

We use the trivial estimate

$$T_p \le \frac{1}{p} \sum_{k \le x/p} \left( \frac{1}{pk+1} + \frac{1}{pk-1} \right) \ll \frac{1}{p^2} \sum_{k \le x} \frac{1}{k} \ll \frac{\log x}{p^2},$$

when $p \ge (\log x)^3$. Thus

$$\begin{aligned} S_1 + S_2 &\le \sum_{\log x < p < (\log x)^3} T_p + \sum_{(\log x)^3 \le p \le x} T_p \\ &\le \sum_{\log x < p} \frac{\log\log x}{p^2} + \sum_{(\log x)^3 \le p} \frac{\log x}{p^2} \\ &\ll \frac{\log\log x}{\log x}, \end{aligned} \tag{7}$$

where we used the trivial bound

$$\sum_{t \le p} \frac{1}{p^2} \le \sum_{t \le n} \frac{1}{n^2} \ll \int_t^\infty \frac{ds}{s^2} = \frac{1}{t}$$

with $t = \log x$ and with $t = (\log x)^3$. Estimates (6) and (7) now lead to the desired conclusion. ∎

*Proof of Proposition 1.* Let $x$ be a large real number and let

$$\mathcal{C}(x) = \{n \le x : \text{if } q \equiv 3 \pmod 4 \text{ and } q^\alpha \,\|\, F_{2n}, \text{ then } \alpha \text{ is even}\}.$$

Lemmas 7 and 8 yield $\#\mathcal{A}(x;5,6) + \#\mathcal{B}(x) = o(x)$. We now show that

$$\mathcal{C}(x) \subset \mathcal{A}(x;5,6) \cup \mathcal{B}(x),$$

which, together with the previous estimate, will prove the proposition. Let $n \in \mathcal{C}(x)$ and assume $n \notin \mathcal{A}(x;5,6)$. Then there exists a prime $p > \log x$ with $p \equiv 5 \pmod 6$ such that $p \mid n$. But $2p \mid 2n$, and $2p \equiv 4 \pmod 6$. Since the Fibonacci sequence is periodic modulo 4 with period 6, and $F_4 = 3$, we find that $F_{2p} \equiv 3 \pmod 4$. Thus, there exists a prime $q \equiv 3 \pmod 4$ such that $q^a \,\|\, F_{2p}$, where $a$ is odd. Since $2p \mid 2n$, we infer that $q^a \mid F_{2n}$. Now since $n \in \mathcal{C}(x)$, we must have $q^{a+1} \mid F_{2n}$. Now $q \mid F_{2n}/F_{2p}$ with $q \mid F_{2p}$ implies, by the well-known law of appearance of powers of primes in Lucas sequences, that $q \mid n/p$. However, since $q \mid F_{2p}$, the rank $\varrho(q)$ is either $p$ or $2p$, which in both cases implies that $q \equiv \pm 1 \pmod p$. Hence, $pq \mid n$, $q \equiv \pm 1 \pmod p$, and $p > \log x$. Therefore, $n \in \mathcal{B}(x)$. This completes our proof. ∎

The following lemma will be useful for the proof of Theorem 3.

LEMMA 9. *Let $d$ be a nonzero integer. Suppose that $p$ is a prime number not dividing $12\varrho(d)$ such that*

$$\left(\frac{d}{F_p}\right) = -1.$$

*Then $\mathcal{N}_d$ is of asymptotic density zero.*

*Proof.* Note that $p \neq 3$, so that $F_p$ is odd and the Jacobi symbol of $d$ with respect to $F_p$ is well-defined. Let $q = 12\varrho(d)k + p$ for some nonnegative integer $k$. By the addition formula $2F_{m+n} = F_m L_n + L_m F_n$, we have

$$2F_q = F_{12\varrho(d)k} L_p + L_{12\varrho(d)k} F_p.$$

Clearly, $16 \mid F_{12} \mid F_{12\varrho(d)k}$ and $d \mid F_{\varrho(d)} \mid F_{12\varrho(d)k}$. Furthermore, since $L_{2n} = 5F_n^2 + 2(-1)^n$,

$$L_{12\varrho(d)k} = 5F_{6\varrho(d)k}^2 + 2$$

is congruent to 2 both modulo 16 and modulo $d$. The above arguments show that

$$2F_q \equiv 2F_p \pmod{\operatorname{lcm}[16,d]},$$

therefore

$$F_q \equiv F_p \pmod{\operatorname{lcm}[8,d]}.$$

These congruences imply the Jacobi symbols' identity

$$\left(\frac{d}{F_q}\right) = \left(\frac{d}{F_p}\right).$$

We now show that $\mathcal{N}_d(x) \subset \mathcal{A}(x; p, 12\varrho(d)) \cup \mathcal{B}(x)$, which will prove that $\#\mathcal{N}_d(x) = o(x)$.

Let $n \in \mathcal{N}_d(x)$ and assume that $n \notin \mathcal{A}(x; p, 12\varrho(d))$, so that there exists a prime $q > \log x$ with $q \mid n$ and $q = 12\varrho(d)k + p$ for some $k \geq 0$. Assume also that $n \notin \mathcal{B}(x)$, so that we now seek a contradiction.

Write $F_q = \delta_q \lambda_q^2$, where $\delta_q$ and $\lambda_q$ are positive integers with $\delta_q$ square-free. Note that $\delta_q$ is odd and $> 1$ because $F_q$ is odd and not a square. Any prime $r$ dividing $\delta_q$ satisfies $r^{\alpha_r} \parallel F_q$ for some odd exponent $\alpha_r$. If $r^{\alpha_r+1} \mid F_n$, then $r \mid F_n/F_q$, and hence $r \mid n/q$, so that $qr \mid n$ and $r \equiv \pm 1 \pmod{q}$ (because $\varrho(r) = q$ and, assuming $\log x \geq 5$, we cannot have $r = q = p = 5$). Thus, $n \in \mathcal{B}(x)$, a contradiction. Therefore $r^{\alpha_r} \parallel F_n$. So, there exist $m, y, z \in \mathbb{N}$ such that

$$y^2 + dz^2 = m\lambda_q^2 \delta_q = F_n, \quad \text{where} \quad \gcd(m, \delta_q) = 1. \tag{8}$$

If $g = \gcd(\delta_q, yz)$, then, having in mind that $\delta_q$ is square-free and $\gcd(\delta_q, d) = 1$ (since $\left(\frac{d}{F_q}\right) = -1 \neq 0$), we get $g \mid \gcd(y, z, \lambda_q)$.

Hence, dividing out relation (8) by $g^2$ yields

$$y_1^2 + dz_1^2 = m\mu_q^2 \delta_q, \tag{9}$$

for some integers $y_1, z_1, \mu_q$ with $\gcd(\delta_q, y_1 z_1) = 1$. But equation (9) implies that $\left(\frac{-d}{\delta_q}\right) = 1$. Because $F_q$ is odd and $F_q = F_{(q-1)/2}^2 + F_{(q+1)/2}^2$, we have $F_q \equiv 1 \pmod{4}$. Therefore

$$-1 = \left(\frac{d}{F_p}\right) = \left(\frac{d}{F_q}\right) = \left(\frac{-d}{F_q}\right) = \left(\frac{-d}{\delta_q}\right) = 1,$$

which is a contradiction, and our proof is complete. ∎

Remark. For $d \in \{\pm 2, \pm 3, \pm 5, \pm 6, \pm 7, \pm 8, \pm 10\}$, $\mathcal{N}_d$ is of asymptotic density 0 since

$$\left(\frac{2}{F_5}\right) = \left(\frac{3}{F_5}\right) = \left(\frac{7}{F_5}\right) = \left(\frac{5}{F_7}\right) = \left(\frac{6}{F_7}\right) = \left(\frac{10}{F_{19}}\right) = -1.$$

In what follows, we put

$$\mathcal{D}_1 = \{d \in \mathcal{D} : d \text{ is square-free}\}.$$

We approach the proof of Theorem 3 by first proving the following somewhat weaker statement.

THEOREM 10. *The estimate*

$$\#\mathcal{D}_1(x) \ll \frac{x}{(\log x)^3}$$

*holds for all sufficiently large values of* $x$.

*Proof.* Let $x$ be large and $y = x^{1/\log\log x}$, $u = \log x/\log y = \log\log x$. Let $\mathcal{D}_2(x) = \{d \in \mathcal{D}_1(x) : |d| \in \Psi(x,y)\}$. By Lemma 6,

$$\#\mathcal{D}_2(x) \le 2\#\Psi(x,y) = 2x\exp(-(1+o(1))u\log u) < \frac{x}{(\log x)^3}, \tag{10}$$

when $x$ is large.

For a positive integer $k$, we write $\omega(k)$ for the number of distinct prime factors of $k$. Let $v = 25(\log\log x)^2$ and put

$$\mathcal{D}_3(x) = \{d \in \mathcal{D}_1(x) : \omega(\varrho(d)) \ge v\}.$$

We now bound $\mathcal{D}_3(x)$. Let $d \in \mathcal{D}_3(x)$. Because $d \mid F_n$ if and only if $\varrho(d) \mid n$, we deduce that $\varrho(d) \mid \prod_{p\mid d} \varrho(p)$. Therefore

$$\varrho(d) \mid \prod_{p\mid d}(p - e_p),$$

where $e_p = \left(\frac{5}{p}\right)$. Since $\omega(\varrho(d)) \ge v$, it follows that either $d$ has at least $w = 5\log\log x$ distinct prime factors, or there exists $p \mid d$ such that $p - e_p$ has at least $w$ distinct prime factors. In the first case, the number of such numbers $d$ does not exceed

$$2\sum_{\substack{m\le x\\ \omega(m)\ge w}} 1 < 2\sum_{\substack{m\le x\\ \omega(m)\ge w}} \frac{x}{m} \le 2x\sum_{k\ge w}\sum_{\substack{m<x\\ \omega(m)=k}} \frac{1}{m}.$$

In the second case, let $p < x$ be a prime such that $p - e_p$ has at least $w$ prime factors. The number of numbers $d$ with $|d| \le x$ which are multiples of $p$ does not exceed

$$\frac{2x}{p} \le \frac{4x}{p - e_p}.$$

Summing up over all such primes and noting that for every $m$ the equation $p - e_p = m$ can have at most two solutions $p$, we find that in this case the number of acceptable $d$'s is

$$\le 8x\sum_{k\ge w}\sum_{\substack{m\le x\\ \omega(m)=k}} \frac{1}{m}.$$

Hence, if we write

$$\mathcal{S}(x;k) = \sum_{\substack{m\le x\\ \omega(m)=k}} \frac{1}{m},$$

then

$$\#\mathcal{D}_3(x) \ll x \sum_{k \geq w} \mathcal{S}(x; k). \tag{11}$$

Using the multinomial formula, we get a bound for $\mathcal{S}(x; k)$:

$$\begin{aligned} \mathcal{S}(x; k) &\leq \frac{1}{k!}\Bigg(\sum_{p \leq x}\sum_{\alpha \geq 1} \frac{1}{p^\alpha}\Bigg)^k = \frac{1}{k!}\Bigg(\sum_{p \leq x} \frac{1}{p} + O(1)\Bigg)^k \\ &= \frac{1}{k!}(\log\log x + O(1))^k. \end{aligned} \tag{12}$$

Furthermore,

$$\frac{(\log\log x + O(1))^k / k!}{(\log\log x + O(1))^{k+1}/(k+1)!} = \frac{k+1}{(\log\log x + O(1))} > 2$$

if $k \geq w$ and $x$ is large, therefore by estimates (11) and (12), and Stirling's formula, we get

$$\begin{aligned} \#\mathcal{D}_3(x) &\ll x \sum_{k \geq w} \mathcal{S}(x; k) \ll \frac{x}{\lfloor w \rfloor !}\,(\log\log x + O(1))^{\lfloor w \rfloor} \\ &\ll x\Bigg(\frac{e \log\log x + O(1)}{w}\Bigg)^w \ll x\Big(\frac{e}{5}\Big)^{5 \log\log x} < \frac{x}{(\log x)^3} \end{aligned} \tag{13}$$

for large $x$ because $5 \log(5/e) = 3.047\ldots > 3$.

Let $\mathcal{D}_4(x) = \mathcal{D}_1(x) \setminus (\mathcal{D}_2(x) \cup \mathcal{D}_3(x))$. Let $d \in \mathcal{D}_4(x)$ and write it as $d = \varepsilon P m$, where $P = P(d) > y$, $m$ is a positive integer $< x/y$, and $\varepsilon \in \{\pm 1\}$. We fix the number $m$ and let $\mathcal{D}_4^m(x)$ be the subset of $\mathcal{D}_4(x)$ that contains the $d$'s for which $d = \pm m P(d)$. Assume $\mathcal{D}_4^m(x)$ is not empty.

Let $z = 300(\log\log x)^2 \log\log\log x$ and let $\mathcal{P} = \{p : p \leq z\}$. For $x$ large, the cardinality of $\mathcal{P}$ satisfies

$$\begin{aligned} \pi(z) &= (1 + o(1))\,\frac{z}{\log z} = 150(1 + o(1))(\log\log x)^2 \\ &> 125(\log\log x)^2 = 5v. \end{aligned}$$

Let $\mathcal{Q}$ be a fixed subset of $\mathcal{P}$ having precisely $5\lfloor v \rfloor$ primes in it. Because $\mathcal{D}_4^m(x)$ is not empty, there is a subset $\mathcal{T}$ of $\mathcal{Q}$ of cardinality $4\lfloor v \rfloor$ such that every prime number in $\mathcal{T}$ is coprime to $12\varrho(m)$. Indeed, since there is a $d$ in $\mathcal{D}_4(x)$ such that $m \mid d$, we know that $\varrho(m)$ divides $\varrho(d)$, so that any $p$ coprime to $12\varrho(d)$ is coprime to $12\varrho(m)$. Thus, let $\mathcal{Q}_m$ be the set of subsets of $\mathcal{Q}$ of cardinality $4\lfloor v \rfloor$ whose (prime) elements are all prime to $12\varrho(m)$. Choose a $\mathcal{T}$ in $\mathcal{Q}_m$ and put $\mathcal{D}_4^{m,\mathcal{T}}(x) = \{d \in \mathcal{D}_4^m(x) : \gcd(p, 12\varrho(d)) = 1,\ \forall p \in \mathcal{T}\}$. We will bound $\mathcal{D}_4(x)$ by using the crude estimate

$$\#\mathcal{D}_4(x) \leq \sum_{m \leq x} \sum_{\mathcal{T} \in \mathcal{Q}_m} \#\mathcal{D}_4^{m,\mathcal{T}}(x).$$

By Lemma 9, we have, for $d \in \mathcal{D}_4^{m,\mathcal{T}}(x)$,

$$\left(\frac{d}{F_p}\right) = 1 \quad \text{for all } p \in \mathcal{T}.$$

The above condition means that

$$\left(\frac{\varepsilon m}{F_p}\right)\left(\frac{P}{F_p}\right) = 1.$$

But again because $p$ is not 3, $F_p$ is odd. And since $F_p$ is the sum of two squares we have $F_p \equiv 1 \pmod 4$, so that

$$\left(\frac{P}{F_p}\right) = \left(\frac{m}{F_p}\right).$$

In the above relation, $m$ is fixed, and $p$ is a prime in the fixed set $\mathcal{T}$. Let again $F_p = \delta_p \lambda_p^2$. The above relation puts $P$ into half of all possible $\phi(\delta_p)$ arithmetic progressions with common differences $\delta_p$, which are all odd and $> 1$. Using the fact that the $F_p$'s are mutually coprime as $p$ varies in $\mathcal{T}$, we conclude that $P$ lies in $1/2^{\#\mathcal{T}}$ of all admissible progressions of the form $A_{\mathcal{T}} \pmod{B_{\mathcal{T}}}$, where

$$B_{\mathcal{T}} = \prod_{p\in\mathcal{T}} \delta_p \le \prod_{p\in\mathcal{T}} F_p \le \exp(\#\mathcal{T} z) = \exp(30000(\log\log x)^4 \log\log\log x). \tag{14}$$

Here, we used the fact that $F_n < e^n$ for all positive integers $n$. By the Brun–Titchmarsh theorem, the number of such primes $P \le x/m$ does not exceed

$$\frac{2x/m}{2^{\#\mathcal{T}} \log(x/mB_{\mathcal{T}})} \le \frac{4x \log\log x}{2^{4\lfloor v\rfloor} m \log x},$$

where we used estimate (14) to conclude that $x/m > y > (B_{\mathcal{T}})^2$ for large $x$, therefore that $x/mB_{\mathcal{T}} > y^{1/2}$. The number of subsets $\mathcal{T} \in \mathcal{Q}_m$ is less than $\binom{5\lfloor v\rfloor}{4\lfloor v\rfloor}$ so that the number of acceptable primes $P$ when $m$ is fixed is

$$\le \frac{1}{2^{4\lfloor v\rfloor}} \binom{5\lfloor v\rfloor}{4\lfloor v\rfloor} \frac{4x\log\log x}{m \log x},$$

and summing up over all possible values of $m$ we get

$$\#\mathcal{D}_4(x) \le \frac{4x\log\log x}{\log x} \cdot \frac{1}{2^{4\lfloor v\rfloor}} \binom{5\lfloor v\rfloor}{4\lfloor v\rfloor} \sum_{m\le x} \frac{1}{m} \ll x\log\log x \cdot \frac{1}{2^{4\lfloor v\rfloor}} \binom{5\lfloor v\rfloor}{4\lfloor v\rfloor}.$$

By Stirling's formula, the above inequality leads, for $x$ large, to

$$\#\mathcal{D}_4(x) \ll x\log\log x \left(\frac{5^5}{4^4\cdot 2^4}\right)^{\lfloor v\rfloor} < \frac{x}{(\log x)^3}, \tag{15}$$

where we used the fact that

$$25\log(5^5/(4^4 \cdot 2^4)) = -6.7644\ldots < -3.$$

The conclusion of the theorem now follows from estimates (10), (13) and (15). ∎

*Proof of Theorem 3.* Let $d \in \mathcal{D}$, and write it as $d = d_1 \cdot d_0^2$, where $d_1$ is square-free. It is clear that $\mathcal{N}_d \subset \mathcal{N}_{d_1}$, therefore $d_1 \in \mathcal{D}$ as well. Thus, if $x$ is large, then

$$\#\mathcal{D}(x) \le \sum_{d_0 \ge 1} \#\mathcal{D}_1(x/d_0^2).$$

By Theorem 10,

$$\#\mathcal{D}(x/d_0^2) \ll \frac{x}{d_0^2(\log(x/d_0^2))^3}.$$

When $d_0 < x^{1/3}$, we have $x/d_0^2 > x^{1/3}$, therefore

$$\#\mathcal{D}(x/d_0^2) \ll \frac{x}{d_0^2(\log x)^3}.$$

Otherwise, we use the trivial inequality $\#\mathcal{D}_1(x/d_0^2) \le 2x/d_0^2$ to get

$$\begin{aligned}\#\mathcal{D}(x) &\ll \sum_{1 \le d_0 \le x^{1/3}} \frac{x}{d_0^2(\log x)^3} + 2\sum_{x^{1/3} \le d_0} \frac{x}{d_0^2} \\ &\ll \frac{x}{(\log x)^3}\sum_{d_0 \ge 1}\frac{1}{d_0^2} + 2x\int_{x^{1/3}}^{\infty}\frac{dt}{t^2} \ll \frac{x}{(\log x)^3},\end{aligned}$$

which completes the proof of the theorem. ∎

## References

[1] J. H. E. Cohn, *Square Fibonacci numbers, etc.*, Fibonacci Quart. 2 (1964), 109–113.
[2] F. Luca, *Prime factors of Fibonacci numbers*, solution to Advanced Problem H546, ibid. 42 (2004).
[3] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge Univ. Press, 1995.

Laboratoire Nicolas Oresme
Université de Caen
F-14032 Caen Cedex, France
E-mail: Christian.Ballot@math.unicaen.fr

Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán, México
E-mail: fluca@matmor.unam.mx

*Received on 1.6.2006*
*and in revised form on 28.10.2006* (5211)