Glasgow Math. J. **49** (2007) 391–403. © 2007 Glasgow Mathematical Journal Trust.
doi:10.1017/S0017089507003734. Printed in the United Kingdom

ON THE SQUARE-FREE PARTS OF $\lfloor en! \rfloor$

FLORIAN LUCA
Instituto de Matemáticas, Universidad Nacional Autonoma de México
C.P. 58089, Morelia, Michoacán, México
e-mail: fluca@matmor.unam.mx

and IGOR E. SHPARLINSKI
Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
e-mail: igor@ics.mq.edu.au

(Received 7 November, 2006; revised 8 March, 2007; accepted 10 March, 2007)

Abstract. In this note, we show that if we write $\lfloor en! \rfloor = s(n)u(n)^2$, where $s(n)$ is square-free then

$$S(N) = \prod_{n \le N} s(n)$$

has at least $C \log\log N$ distinct prime factors for some absolute constant $C > 0$ and sufficiently large N. A similar result is obtained for the total number of distinct primes dividing the mth power-free part of $s(n)$ as n ranges from 1 to N, where $m \ge 3$ is a positive integer. As an application of such results, we give an upper bound on the number of $n \le N$ such that $\lfloor en! \rfloor$ is a square.

2000 *Mathematics Subject Classification.* 11B83, 11D41, 11N36.

1. Introduction. Write $A_0 = 1$ and $A_n = \lfloor en! \rfloor$ for $n \ge 1$. Since

$$e = \sum_{k=0}^{\infty} \frac{1}{k!},$$

it follows easily that

$$A_n = \sum_{k=0}^{n} \frac{n!}{k!} \qquad \text{for all } n \ge 0. \tag{1}$$

Using (1), one deduces easily the recurrence $A_n = nA_{n-1} + 1$ for all $n \ge 1$.

For a positive integer m we put $\omega(m)$ for the number of distinct prime factors of m. In [**1**], it has been shown that if we put

$$Q(N) = \prod_{n \le N} A_n,$$

then the inequality

$$\omega(Q(N)) \ge (1/2 + o(1)) \frac{N}{\log N}$$

holds as $N \to \infty$. In this paper, we fix $m \geq 2$ and write $A_n = s_m(n)u_m(n)^m$ for some integer $s_m(n)$ and $u_m(n)$ where $s_m(n)$ is free of m powers (that is, p^m does not divide $s_m(n)$ for any prime number p). Then we study the number of distinct prime factors of

$$S_m(N) = \prod_{n \leq N} s_m(n).$$

It has been shown in [**1**, Theorem 5] that $\omega(S_2(N))$ tends to infinity with N but the argument used there is ineffective. While we certainly believe that $\omega(S_m(N)) \gg N$ holds as $N \to \infty$, we can only prove much weaker results. In fact, we derive out estimates on $\omega(S_m(N))$ from lower bounds on the cardinality of the set

$$\mathcal{S}_m(N) = \{s_m(n) \ : \ n \leq N\}$$

and the trivial inequality

$$\#\mathcal{S}_m(N) \leq m^{\omega(S_m(N))}. \tag{2}$$

Note that $\#\mathcal{S}_m(N)$ is exactly the number of distinct fields $\mathbb{Q}(A_n^{1/m})$, $n \leq N$.

THEOREM 1. (i) *The inequality*

$$\#\mathcal{S}_2(N) \geq (\log N)^{1/3+o(1)}$$

holds as $N \to \infty$.

(ii) *The inequality*

$$\#\mathcal{S}_m(N) \geq N^{1/(2m)+o(1)}$$

holds uniformly for $3 \leq m \leq \log N/\log\log N$ *as* $N \to \infty$.

Using (2), we deduce:

COROLLARY 1. (i) *The inequality*

$$\omega(S_2(N)) \geq \left(\frac{1}{3\log 2} + o(1)\right)\log\log N$$

holds as $N \to \infty$.

(ii) *The inequality*

$$\omega(S_m(N)) \geq \left(\frac{1}{2m\log m} + o(1)\right)\log N$$

holds uniformly for $3 \leq m \leq \log N/\log\log N$ *as* $N \to \infty$.

As an application, we estimate the number of $n \leq N$ such that $\lfloor en! \rfloor = m^2$ for some positive integer m. We put

$$\mathcal{T}(N) = \{n \leq N : \lfloor en! \rfloor = m^2 \text{ for some positive integer } m\}.$$

THEOREM 2. *The estimate*

$$\#\mathcal{T}(N) \leq N \exp\left(-(1/6\log 2 + o(1))\log\log N \log\log\log\log N\right)$$

holds as $N \to \infty$.

https://doi.org/10.1017/S0017089507003734 Published online by Cambridge University Press

We conjecture that $\mathcal{T}$ is finite but have no idea how to prove such a fact.

Throughout the paper, the implied constants in the symbols 'O', '$\ll$' and '$\gg$' are absolute. We recall that the notations $U = O(V)$, $U \ll V$, and $V \gg U$ are all equivalent to the assertion that the inequality $|U| \leq cV$ holds for some constant $c > 0$.

2. Preliminary results. We need the following congruences involving $(A_n)_{n\geq 0}$.

LEMMA 1. *If $n \geq k \geq 0$ are integers then*

$$A_n \equiv A_k \pmod{n-k}.$$

Proof. Applying the definition it is immediate that

$$\begin{aligned} A_n &= \sum_{j=0}^{n} \frac{n!}{j!} = \sum_{j=0}^{n-k-1} \frac{n!}{j!} + \sum_{j=n-k}^{n} \frac{n!}{j!} \\ &= n(n-1)\cdots(n-k)A_{n-k-1} + \sum_{i=0}^{k} \frac{n!}{(n-i)!}. \end{aligned} \tag{3}$$

Reducing the relation (3) modulo $n-k$ and using the fact that $n!/(n-i)! \equiv k!/(k-i)!$ (mod $n-k$) for all $i = 1, \ldots, k$, we get that

$$A_n \equiv \sum_{i=0}^{k} \frac{k!}{(k-i)!} \equiv A_k \pmod{n-k},$$

which completes the proof of this lemma. □

We also need the following multiplicative independence property of non-torsion units of mutually distinct quadratic fields.

LEMMA 2. *Let $k \geq 1$ be a positive integer and $d_1, \ldots, d_k$ be square-free positive integers such that for each $i = 1, \ldots, k$, there exists a prime number $p_i | d_i$ such that $p_i \nmid d_j$ for any $j < i$. Assume further that α_i is a unit in the quadratic field $\mathbb{Q}[\sqrt{d_i}]$ with $\alpha_i > 1$ for $i = 1, \ldots, k$. If a_i, $i = 1, \ldots, k$, are integers such that*

$$\prod_{i=1}^{k} \alpha_i^{a_i} = 1, \tag{4}$$

then $a_i = 0$ for all $i = 1, \ldots, k$.

Proof. By replacing simultaneously the $\alpha_1, \ldots, \alpha_k$ by their squares, we may assume that each α_i is a unit of norm 1 in the corresponding quadratic field $\mathbb{Q}[\sqrt{d_i}]$ for all $i = 1, \ldots, k$.

We now proceed by induction on k, the case $k = 1$ being obvious. Since $p_k | d_k$ but $p_k \nmid d_i$ for any $i < k$, it follows easily that the fields $\mathbb{K} = \mathbb{Q}[\sqrt{d_k}]$ and $\mathbb{L} = \mathbb{Q}[\sqrt{d_1}, \ldots, \sqrt{d_{k-1}}]$ have $\mathbb{K} \cap \mathbb{L} = \mathbb{Q}$. It now follows that there exists a Galois automorphism of $\mathbb{F} = \mathbb{Q}[\sqrt{d_1}, \ldots, \sqrt{d_k}]$, let us call it σ, such that $\sigma(\sqrt{d_k}) = -\sqrt{d_k}$ and $\sigma(\sqrt{d_i}) = \sqrt{d_i}$ for all $i = 1, \ldots, k-1$. Conjugating the relation (4) by σ and using the

https://doi.org/10.1017/S0017089507003734 Published online by Cambridge University Press

fact that $\sigma(\alpha_k) = \alpha_k^{-1}$ and $\sigma(\alpha_i) = \alpha_i$ for $i = 1, \ldots, k-1$, we get that

$$\alpha_1^{a_1} \ldots \alpha_{k-1}^{a_{k-1}} \alpha_k^{-a_k} = 1,$$

which together with the equation (4) leads to $\alpha_k^{2a_k} = 1$, therefore $a_k = 0$ since $\alpha_k > 1$. Hence, in the relation (4), we may assume that α_k is not present. Now we may apply the induction hypothesis. □

We also need the following results from Diophantine equations. The first one is due to Bennett [**2**].

LEMMA 3. *Let a, b and m be fixed positive integers with $m \geq 3$. Then the Diophantine equation*

$$ax^m - by^m = 1$$

has at most one solution in positive integers x and y.

The second one is a result from the theory of $\mathcal{S}$-unit equations. Let $\mathbb{K}$ be any algebraic number field of degree d. For $\pi_1, \ldots, \pi_s \in \mathbb{K}$ we let

$$\mathcal{S} = \{\pi_1^{\alpha_1} \ldots \pi_s^{\alpha_s} : \alpha_1, \ldots, \alpha_s \in \mathbb{Z}\}.$$

The algebraic numbers in $\mathcal{S}$ are usually called $\mathcal{S}$-*units*. Let $k \geq 2$ be fixed. Consider the equation

$$\sum_{i=1}^{k} x_i = 0, \tag{5}$$

where $x_i \in \mathcal{S}$ for all $i = 1, \ldots, k$. Such an equation is usually referred to as an $\mathcal{S}$-unit equation. A solution $\mathbf{x} = (x_1, \ldots, x_k)$ is called non-degenerate if $\sum_{i \in I} x_i \neq 0$ for all proper non-empty subsets I of $\{1, \ldots, k\}$. The following result is Theorem 1.1 in [**4**].

LEMMA 4. *There exists a computable constant $C(k, s)$, depending only on k and s and a set of non-degenerate solutions $\mathcal{T} = \{\mathbf{x}_1, \ldots, \mathbf{x}_t\} \subseteq \mathbb{K}^t$ of the $\mathcal{S}$-unit equation* (5) *with $t \leq C(k, s)$, such that if $\mathbf{x}$ is any non-degenerate solution of the $\mathcal{S}$-unit equation* (5)*, then there exists $j \leq t$ and $\rho \in \mathcal{S}$ such that $\mathbf{x} = \rho \mathbf{x}_j$.*

In [**4**], it is shown that one can take

$$C(k, s) = \exp\left(6(k+1)^{3(k+1)}(s+1)\right),$$

but we shall not need this.

3. Proof of Theorem 1.

3.1. Part (i). For simplicity, we write $s(n)$, $u(n)$ and $\mathcal{S}(N)$ instead of $s_2(n)$, $u_2(n)$ and $\mathcal{S}_2(N)$, respectively. We start by noting that $A_8 = 109601 = 127 \cdot 863$ and $A_9 = 986410 = 2 \cdot 5 \cdot 98641$ are both square-free. For a positive integer t let $(X_t, Y_t)_{t \geq 1}$ be the t-th solution of the Pell equation

$$X^2 - 2Y^2 = 1,$$

https://doi.org/10.1017/S0017089507003734 Published online by Cambridge University Press

where we order them, as usually, in increasing order according to the size of X. Note that $(X_1, Y_1) = (3, 2)$. We now let $\mathcal{A}$ be the set of odd positive integers t such that $X_t \equiv 3 \pmod{(A_8A_9)^2}$. Note that $\mathcal{A}$ is infinite because the sequence $(X_t)_{t\geq 1}$ is periodic modulo m for every fixed positive integer m and $X_1 = 3$. Thus, if L denotes the period of the sequence $(X_t)_{t\geq 1}$ modulo $(A_8A_9)^2$, then $\mathcal{A}$ contains all positive integers $t \equiv 1 \pmod{2L}$. We now consider the set

$$\mathcal{N} = \left\{n = X_t^2 \leq N \ : \ n > \log\log N \text{ and } t \in \mathcal{A}\right\}.$$

Since

$$X_t = \frac{1}{2}((3 + 2\sqrt{2})^t + (3 - 2\sqrt{2})^t) < (3 + 2\sqrt{2})^t,$$

it follows that all $t \leq \log(\sqrt{N})/\log(3 + 2\sqrt{2})$ in the arithmetical progression $t \equiv 1 \pmod{2L}$ lead to $n = X_t^2 \in \mathcal{N}$. Hence, $\#\mathcal{N} \gg \log N$.

If we put

$$(s(n), s(n-1), s(n-2)) = (d_1, d_2, d_3)$$

and

$$(u(n), u(n-1), u(n-2)) = (x_1, x_2, x_3),$$

then relation $A_k = kA_{k-1} + 1$ for $k = n$ and $n - 1$ becomes

$$d_1x_1^2 - d_2(ux_2)^2 = 1 \tag{6}$$

and

$$d_2x_2^2 - (2d_3)(vx_3)^2 = 1, \tag{7}$$

respectively, for certain positive integers u and v with $u^2 - 2v^2 = 1$. We now make some comments about d_1, d_2 and d_3. Since

$$A_n = nA_{n-1} + 1 = n(n-1)A_{n-2} + n + 1 \equiv n + 1 \pmod 2$$

and n is odd (because $n - 1 = 2v^2$ is even), we get that A_n is even and A_{n-1} is odd. Hence, d_2, u and x_2 are all odd. Now note that $p = 98641$ is a prime and that $p|A_9$.

Lemma 1 with $k = 9$ (note that $n > 9$ if N is large) gives

$$A_n \equiv A_9 \pmod{n-9},$$

and since $n - 9 = (X_t - 3)(X_t + 3)$ is a multiple of p^2 and $p|A_9$, we get that $p\|A_n$ (where as usual, for a prime ℓ, $\ell \parallel a$ means that $\ell \,|\, a$ and $\ell^2 \nmid a$). Hence, $p \,|\, d_1$. By the same argument, taking the prime factor $q = 127$ of A_8, we have, since

$$A_{n-1} \equiv A_8 \pmod{n-9},$$

and since $n - 9 = (X_t - 3)(X_t + 3)$ is also a multiple of A_8^2, that $q^2 \mid (n - 9)$. Since A_8 is square-free, we get that $q \parallel A_{n-1}$, therefore $q \mid d_2$. Note that $q \nmid A_n$ because from $A_n = nA_{n-1} + 1$ we read that A_n and A_{n-1} are coprime. We also note that p does not

https://doi.org/10.1017/S0017089507003734 Published online by Cambridge University Press

divide A_{n-2} because from the relation $A_n = n(n-1)A_{n-2} + n + 1$ we deduce that if $p \mid A_{n-2}$, then $p \mid (n+1)$, which is false because $p \mid (n-9)$ and $p > 10$. Thus, we have

$$p \mid d_1, \qquad p \nmid d_2 d_3, \qquad q \mid d_2, \qquad q \nmid d_1 d_3. \tag{8}$$

Now let (U_1, V_1) and (W_1, Z_1) be smallest positive integer solution of the equations

$$d_1 U^2 - d_2 V^2 = 1, \tag{9}$$

and

$$d_2 W^2 - 2 d_3 Z^2 = 1, \tag{10}$$

respectively.

We put

$$\alpha = \sqrt{d_1} U + \sqrt{d_2} V \qquad \text{and} \qquad \beta = \sqrt{d_2} W + \sqrt{2 d_3} Z.$$

It is well-known by the theory of Pell equations (see, for example, Nagell's paper [7]), that all the positive integer solutions (U_ℓ, V_ℓ) of the equation (9) arise from

$$\sqrt{d_1} U_\ell + \sqrt{d_2} V_\ell = \alpha^\ell \qquad \text{for some odd } \ell,$$

and all the positive integer solutions (W_r, Z_r) of the equation (10) arise from

$$\sqrt{d_2} W_r + \sqrt{2 d_3} Z_r = \beta^r \qquad \text{for some odd } r,$$

respectively. Hence, comparing the above relations with (6) and (7) respectively, we get that

$$u x_2 = \frac{\alpha^\ell - \alpha^{-\ell}}{2\sqrt{d_2}}, \tag{11}$$

and

$$x_2 = \frac{\beta^r + \beta^{-r}}{2\sqrt{d_2}}. \tag{12}$$

Note also that since $u = X_t$, we get that

$$u = \frac{\gamma^t + \gamma^{-t}}{2}, \tag{13}$$

where $\gamma = 3 + 2\sqrt{2}$. Identifying x_2 from (11) and (12) and using also the relation (13), we get

$$(\gamma^t + \gamma^{-t})(\beta^r + \beta^{-r}) = 2(\alpha^\ell - \alpha^{-\ell}). \tag{14}$$

Since $\#\mathcal{N} \gg \log N$ but

$$\#\{(d_1, d_2, d_3) \ : \ n \in \mathcal{N}\} \le (\#\mathcal{S}(N))^3,$$

we get that there exists one triple (d_1, d_2, d_3) such that (14) has at least

$$M \ge (\#\mathcal{S}(N))^{-3} \#\mathcal{N} \gg (\#\mathcal{S}(N))^{-3} \log N \tag{15}$$

https://doi.org/10.1017/S0017089507003734 Published online by Cambridge University Press

solutions (t, r, l), where α, β and γ are of course uniquely determined in terms of (d_1, d_2, d_3).

We now note that the equation (14) can be rewritten as

$$X_1 + X_2 + X_3 + X_4 + X_5 + X_6 = 0,$$

with

$$X_1 = \gamma^t \beta^r, \qquad X_2 = \gamma^t \beta^{-r}, \qquad X_3 = \gamma^{-t} \beta^r,$$
$$X_4 = \gamma^{-t} \beta^{-r}, \qquad X_5 = -2\alpha^\ell, \qquad X_6 = 2\alpha^{-\ell},$$

which is an $\mathcal{S}$-unit equation for which

$$\mathcal{S} = \{-1, 2, \alpha, \beta, \gamma\}$$

has $s = 5$ and $k = 6$.

We note that $\alpha^2 \in \mathbb{Q}(\sqrt{d_1 d_2})$, $\beta^2 \in \mathbb{Q}(\sqrt{d_2 d_3})$ and $\gamma^2 \in \mathbb{Q}(\sqrt{2})$ are multiplicatively independent by Lemma 2 and our choice of primes p and q, see (8). Therefore α, β and γ are also multiplicatively independent.

Here, $\mathbb{K} = \mathbb{Q}[\alpha, \beta, \gamma]$ has degree $d = 8$. Further, note that $t > 0$ for large N because $u = n^{1/2} \gg (\log\log N)^{1/2}$. We now show that the above equation has only at most $O(1)$ solutions. Indeed, let $\mathcal{J} \subseteq \{1, \ldots, 6\}$ be a subset of minimal cardinality $J = \#\mathcal{J}$ such that

$$\sum_{j \in \mathcal{J}} X_j = 0$$

and this sub-equation is non-degenerate. Clearly, $J > 1$. If $J = 2$, then

- either $\pm 2\alpha^a = \beta^b \gamma^c$, where $a \in \{\pm l\}$, $b \in \{\pm r\}$, $c \in \{\pm t\}$, which is impossible because α, β, γ are units but 2 is not;
- or $\alpha^\ell = \alpha^{-\ell}$, which is impossible because $\ell > 0$ and $\alpha > 1$;
- or $\beta^{b_1} \gamma^{c_1} = \beta^{b_2} \gamma^{c_2}$, where $b_1, b_2 \in \{\pm r\}$, $c_1, c_2 \in \{\pm t\}$, which is impossible because it leads to a non-trivial multiplicative relation on β^2 and γ^2 which, as we have mentioned, cannot exist by Lemma 2 and (8).

Thus, either $J = 3$, or $J = 6$. If $J = 3$, then, replacing $\mathcal{J}$ with its complement we see that we can assume that either 5 or 6 belongs to $\mathcal{J}$. Further, since $J \geq 3$, there exists $j \leq 4$ in $\mathcal{J}$. From now on, we assume that $\mathcal{J}$ contains at least one element among the first four and at least one other among the last two. Lemma 4 now shows that there exist at most $M_{\mathcal{J}} \leq C(J, 5)$ solutions $\mathbf{X}_i = (X_{j,i})_{j \in \mathcal{J}}$, $i = 1, \ldots, M_{\mathcal{J}}$, such that if $\mathbf{X} = (X_j)_{j \in \mathcal{J}}$ is any other solution, we then have that $X_j = \rho X_{j,i}$ for all $j \in \mathcal{J}$, some $\rho \in \mathcal{S}$ and $i \in \{1, \ldots, M_{\mathcal{J}}\}$, which we write as

$$\frac{X_{j,i}}{X_j} = \rho, \qquad j \in \mathcal{J}.$$

Let $j_1 < j_2$ be the smallest and largest elements in $\mathcal{J}$, respectively. We saw that $j_1 \leq 4$. Then the above relation shows that

$$\frac{X_{j_1,i}}{X_{j_1}} = \frac{X_{j_2,i}}{X_{j_2}}.$$

https://doi.org/10.1017/S0017089507003734 Published online by Cambridge University Press

If we write $X_{j_1,i} = \beta^{b_i}\gamma^{c_i}$, $X_{j_1} = \beta^b\gamma^c$, $X_{j_2,i} = 2\varepsilon\alpha^{a_i}$, $X_{j_2} = 2\varepsilon\alpha^a$, where $\varepsilon \in \{\pm 1\}$, we get that

$$\beta^{b_i-b}\gamma^{c_i-c} = \alpha^{a_i-a}.$$

Since, as we have mentioned, α, β and γ are multiplicatively independent (by Lemma 2 and (8)), we get that $a_i = a$, $b_i = b$ and $c_i = c$, implying that $\rho = 1$. Thus, the equation (14) has at most

$$M \le \sum_{\substack{\mathcal{J}\subseteq\{1,\dots,6\}\\ \#\mathcal{J}=3,\ 6}} C(\#\mathcal{J}, 5) = O(1) \tag{16}$$

solutions. Comparing (15) and (16), we obtain the bound of Part (i) of Theorem 1.

3.2. Part (ii). Part (ii) is much easier. For this, we take $\mathcal{A}$ to be the set of all $n = u^m \le N$ with some integer u.

The number of such n is

$$\#\mathcal{A} \ge \left\lfloor N^{1/m} \right\rfloor \ge 0.5N^{1/m},$$

uniformly in the given range for m when N is large.

Let now $s = \omega(S_m(N))$. For each $n \in \mathcal{A}$, we write $(s_m(n), s_m(n-1)) = (d_1, d_2)$. Clearly, the pair (d_1, d_2) can take at most $(\#\mathcal{S}_m(N))^2$ values. For each such fixed pair, the equation $A_n - nA_{n-1} = 1$ (with $n = u^m \in \mathcal{A}$) leads to the positive integer solution $(X, Y) = (u(n), u(n-1))$ of the Diophantine equation $d_1X^m - d_2Y^m = 1$. By Lemma 3, this solution is unique. Hence,

$$(\#\mathcal{S}_m(N))^2 \ge \#\mathcal{A},$$

which completes the proof of Part (ii) of Theorem 1.

4. Proof of Theorem 2. We follow the method of proof of Theorem 5 in [**1**], except that instead of the Brun sieve we use the large sieve. We also use Theorem 1 in a substantial way. We also continue to use $s(n)$, $u(n)$ and $\mathcal{S}(N)$ instead of $s_2(n)$, $u_2(n)$ and $\mathcal{S}_2(N)$, respectively.

Let us fix an arbitrary $\varepsilon > 0$ and put

$$M = \left\lfloor \frac{\log\log N}{\log\log\log N \log\log\log\log N} \right\rfloor \qquad \text{and} \qquad K = \left\lfloor \frac{1-\varepsilon}{3\log 2} \log\log M \right\rfloor.$$

Thus,

$$2^K \le \#\mathcal{S}(M)$$

provided that N is large enough.

Let $\mathcal{P}(M)$ be the set of all prime divisors of $S(M) = s(1)\cdots s(M)$. Each factorization

$$s = \prod_{p\in\mathcal{P}(M)} p^{\alpha_{p,s}}, \qquad s \in \mathcal{S}(M),$$

https://doi.org/10.1017/S0017089507003734 Published online by Cambridge University Press

defines a distinct binary vectors $(\alpha_{p,s})_{p\in\mathcal{P}(M)}$. We now choose the sequence of integers $1 = i_1 < \cdots < i_K$ inductively as follows.

- We put $i_1 = 1$.
- Assume that $i_1 < \cdots < i_k$ are chosen and $k < K$. We define i_{k+1} as the smallest integer for which $s(i_{k+1}) \in \mathcal{S}(M)$ and such that the vector $(\alpha_{p,s(i_{k+1})})_{p\in\mathcal{P}(M)}$ does not belong to the linear space over the finite field $\mathbb{F}_2$ of two elements generated by the vectors

$$(\alpha_{p,s(i_1)})_{p\in\mathcal{P}(M)}, \dots, (\alpha_{p,s(i_k)})_{p\in\mathcal{P}(M)}.$$

Clearly this is possible as long as $2^k < 2^K \le \#\mathcal{S}(M)$.

Note that the product

$$D = \prod_{j=1}^{K} s(i_j)$$

satisfies the inequality

$$D \le A_M^K \le ((M+1)!)^K = \exp\left((1/3 + o(1))M \log M \log\log M\right) \le \log N, \quad (17)$$

provided that N is large enough.

For an integer a and an odd positive integer m we use $(a \mid m)$ to denote the Jacobi symbol of a with respect to m.

Let $n \in \mathcal{T}(N)$, and let $j \in \{1, \dots, K\}$. Then, by Lemma 1, we have

$$A_n \equiv A_{i_j} \equiv s(i_j)u(i_j)^2 \pmod{n - i_j},$$

and so we conclude that every prime factor $p > \log N > A_M$ of $n - i_j$ must have the property that $(s(i_j) \mid p) = 1$. For each $j = 1, \dots, K$, we write

$$\mathcal{R}_j = \{p > \log N \ : \ (s(b_{i_j}) \mid p) = -1\},$$

and so we conclude that $n - i_j$ is free of primes $p \in \mathcal{R}_j$. Thus,

$$\mathcal{T}(N) \subseteq \bigcap_{j=1}^{M} \{n \le N \ : \ n - i_j \text{ is free of primes } p \in \mathcal{R}_j\}. \quad (18)$$

To estimate the cardinality of the set appearing in the right-hand side above, we use the large sieve. Recall that the arithmetic form of the *large sieve inequality* (see, for example, [**8**, Section I.4.5, Corollary 6.1]), states that for any finite sequence of complex numbers $\{b_n \ : \ X < n \le X + Y\}$, the bound

$$\left| \sum_{X<n\le X+Y} b_n \right|^2 \le \frac{Y - 1 + Q^2}{L} \sum_{X<n\le X+Y} |b_n|^2 \quad (19)$$

https://doi.org/10.1017/S0017089507003734 Published online by Cambridge University Press

holds, where

$$Q \ge 1, \qquad L = \sum_{k \le Q} |\mu(k)| \prod_{p \mid k} \frac{w(p)}{p - w(p)},$$

$\mu(k)$ is the Möbius function and, for every prime p,

$$w(p) = \#\{h \ : \ 0 \le h < p, \ n \equiv h \pmod p \implies b_n = 0\}.$$

We put $Q = N^{1/2}$, and define

$$b_n = \begin{cases} 1 & \text{if } n - i_j \text{ is free of primes } p \in \mathcal{R}_j \text{ for } j = 1, \ldots, K, \\ 0 & \text{otherwise.} \end{cases}$$

We also put $w(p) = 0$ for $p \le \log N$ and

$$w(p) = \#\{j \in \{1, \ldots, K\} \ : \ (s(i_j) \mid p) = -1\},$$

for $p > \log N$.

Note that if $p > \log N > M$, then $i_1 < \cdots < i_K \le M$ are all distinct residues modulo p. Then taking $X = Q$ and $Y = Q^2 - Q$ in (19) and using (18), we see that

$$\begin{aligned} \#\mathcal{T}(N) &\le Q + \sum_{Q < n \le Q^2} b_n \le Q + \frac{(Q^2 - Q) - 1 + Q^2}{L} \\ &\ll Q + \frac{Q^2}{L} = \frac{N}{L} + N^{1/2}. \end{aligned} \tag{20}$$

It remains to find a lower bound for L. We put $X = N^{1/(\log\log N)^2}$ and note that

$$L = L_1 + L_2 - L_3,$$

where

$$\begin{aligned} L_1 &= \prod_{p \le X} \left(1 + \frac{w(p)}{p - w(p)}\right), \\ L_2 &= \sum_{\substack{k \le N^{1/2} \\ P(k) > X}} |\mu(k)| \prod_{p \mid k} \frac{w(p)}{p - w(p)}, \\ L_3 &= \sum_{\substack{k > N^{1/2} \\ P(k) \le X}} |\mu(k)| \prod_{p \mid k} \frac{w(p)}{p - w(p)}. \end{aligned}$$

Since $w(p) \le K \ll \log\log\log\log N$ we conclude that $p - w(p) \ge p/2$ for all $p > \log N$ whenever N is large, and, since also $\omega(k) > (\log\log N)^2/2$ whenever $k > N^{1/2}$

https://doi.org/10.1017/S0017089507003734 Published online by Cambridge University Press

is square-free and $P(k) \le X$, we get that

$$\begin{aligned}
L_3 &\le \sum_{\substack{P(k)\le X \\ \omega(k)\ge (\log\log N)^2/2}} \mu(k)^2 \frac{(2K)^{\omega(k)}}{k} \\
&\le \sum_{\omega \ge (\log\log N)^2/2} \sum_{\substack{P(k)\le X \\ \omega(k)=\omega}} \mu(k)^2 \frac{(2K)^{\omega}}{k} \\
&\le \sum_{\omega \ge (\log\log N)^2/2} \frac{(2K)^{\omega}}{\omega!} \left(\sum_{p\le X} \frac{1}{p} \right)^{\omega} \\
&\le \sum_{\omega \ge (\log\log N)^2/2} \frac{(2K)^{\omega}}{\omega!} (\log\log X + O(1))^{\omega} \\
&\le \sum_{\omega \ge (\log\log N)^2/2} \left(\frac{2eK(\log\log N + O(1))}{\omega} \right)^{\omega} \\
&\ll \sum_{\omega \ge (\log\log N)^2/2} \left(\frac{4eK(\log\log N + O(1))}{(\log\log N)^2} \right)^{\omega} \\
&\ll \exp\left(-(1/2 + o(1))(\log\log N)^2 \log\log\log N \right).
\end{aligned}$$

In the above estimates, we used the known inequality $\omega! \ge (\omega/e)^{\omega}$, as well as the fact that the estimate

$$\sum_{p\le y} \frac{1}{p} = \log\log y + O(1)$$

holds as $y \to \infty$. Hence, $L_3 = o(1)$, $L_2 \ge 0$ and $L_1 \ge 1$, therefore

$$L \ge (1 + o(1))L_1 \tag{21}$$

as $N \to \infty$. Clearly,

$$\begin{aligned}
L_1 &= \exp\left(\sum_{p\le X} \log\left(1 + \frac{\omega(p)}{p - \omega(p)} \right) \right) \\
&= \exp\left(\sum_{p\le X} \frac{w(p)}{p - w(p)} + O\left(\sum_{p\ge X} \left(\frac{w(p)}{p - w(p)} \right)^2 \right) \right) \\
&= \exp\left(\sum_{p\le X} \frac{w(p)}{p} + O\left(\sum_{p\ge \log N} \frac{K^2}{p^2} \right) \right) \\
&= \exp\left(\sum_{p\le X} \frac{w(p)}{p} + O\left(\frac{K^2}{\log N} \right) \right) \\
&= (1 + o(1)) \exp\left(\sum_{p\le X} \frac{w(p)}{p} \right).
\end{aligned}$$

https://doi.org/10.1017/S0017089507003734 Published online by Cambridge University Press

Thus, recalling the estimates (20) and (21), we get

$$\#\mathcal{T}(N) \le (1+o(1))N \exp\left(-\sum_{p\le X}\frac{w(p)}{p}\right) + O\big(N^{1/2}\big). \tag{22}$$

We now remark that it has been shown in the proof of Theorem 5 in [**1**], that

$$\sum_{p<X}\frac{w(p)}{p} = (1/2+o(1))K\log\log N. \tag{23}$$

More precisely, in [**1**] K has been fixed but it is trivial to check that the result holds under the condition (17) which is implied by the above choice of K and M.

Now the bound (23), together with the estimate (22) and the fact that ε is arbitrarily small, implies the conclusion of Theorem 2.

5. Comments and remarks. With minor modifications, the results obtained in this paper apply to other sequences of positive integers satisfying similar recurrences, like sequences $(U_n)_{n\ge 1}$ satisfying a recurrence of the shape $U_n = f(n)U_{n-1} + B_n$, where $f(n)$ is a nonconstant polynomial with integer coefficients and B_n is a bounded periodic sequence of integers. In particular, they apply to the sequence of general term $A_n = \lfloor n!/e \rfloor$. Furthermore, all our arguments can be made completely explicit, but this is beyond the purpose of the present paper. We remark that arithmetical properties of sequences of integers satisfying linear recurrence relations with constant coefficients have been the subject of extensive investigation (see [**3**] for the state of the art in this subject). In particular, there are several known facts about prime divisors of members of such sequences, or whether such sequences contain infinitely many perfect squares. Much less is known about arithmetical properties of sequences of positive integers satisfying linear recurrences with polynomial coefficients, like the one treated in this paper, although some general results may be found in the recent papers [**5**] and [**6**].

ACKNOWLEDGEMENTS. We thank the referee for a careful reading of our manuscript and for suggesting changes which improved the quality of this paper. This work was done in April of 2006, while the first author was in residence at the Centre de Recherches Mathématiques of the Université de Montréal for the thematic year *Analysis and Number Theory*. This author thanks the organizers for the opportunity of participating in this program. During the preparation of this paper, F. L. was also supported in part by grants PAPIIT IN104505, SEP-CONACyT 46755 and a Guggenheim Fellowship and I. S. was supported in part by ARC grant DP0556431.

REFERENCES

1. S. Balasurya, F. Luca and I. E. Shparlinski, Prime divisors of some recurrence sequence, *Per. Math. Hungarica*, to appear.

2. M. A. Bennett, Rational approximations to algebraic numbers of small height: the Diophantine equation $|ax^n - by^n| = 1$, *J. Reine Angew. Math.* **535** (2001), 1–49.

3. G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, *Recurrence sequences*, Mathematical Surveys and Monographs **104** (Amer. Math. Soc., Providence, RI, 2003).

4. J.-H. Evertse, H. P. Schlickewei and W. M. Schmidt, Linear equations in variables which lie in a multiplicative group, *Ann. Math.* **155** (2002), 807–836.

5. M. Z. Garaev, F. Luca and I. E. Shparlinski, Catalan and Apéry numbers in residue classes, *J. Combin. Theory Ser. A* **113** (2006), 851–865.

6. F. Luca, Prime divisors of binary holonomic sequences, *Advances in App. Math.*, to appear.

7. T. Nagell, On a special class of Diophantine equations of the second degree, *Ark. Mat.* **3** (1954), 51–65.

8. G. Tenenbaum, *Introduction to analytic and probabilistic number theory* (Cambridge University Press, 1995).