ON SQUARE VALUES OF THE PRODUCT OF THE EULER TOTIENT AND SUM OF DIVISORS FUNCTIONS

KEVIN BROUGHAN, KEVIN FORD, AND FLORIAN LUCA

ABSTRACT. If n is a positive integer such that $\phi(n)\sigma(n) = m^2$ for some positive integer m, then $m \leqslant n$. We put $m = n - a$ and we study the positive integers a arising in this way.

Keywords: sum of divisors, Euler function.

AMS Subject Classification: 11A41.

1 Introduction

It is known (e.g. [3] and [11]), and we will revisit this argument shortly, that there are infinitely many positive integers n such that $\phi(n)\sigma(n) = \square$[1]. Here, we look at such positive integers n. Clearly, $n = 1$ has the property. Suppose that $n > 1$ and write its prime factorization as

eq:1 (1.1)
$$n = \prod_{i=1}^{k} p_i^{\alpha_i}.$$

Then

eq:2 (1.2)
$$\frac{\phi(n)\sigma(n)}{n^2} = \prod_{i=1}^{k}\left(1 - \frac{1}{p_i^{\alpha_i+1}}\right).$$

Thus, if $n > 1$ and $\phi(n)\sigma(n) = m^2$ for some positive integer m, then $m < n$, so we can write $m = n - a$ for some positive integer a. In this paper, we look at the positive integers a arising in this way. First, we fix such a number a and study the set

$$\mathcal{N}_a := \{n : n > a \text{ and } \phi(n)\sigma(n) = (n-a)^2\}.$$

It is easy to see that each $n \in \mathcal{N}_a$ has the same parity as a. Our first result shows that $\mathcal{N}_a$ is a finite set.

thm:1 **Theorem 1.** *All elements n in $\mathcal{N}_a$ have $\omega(n) > 1$ and $n \leqslant 2a^3$.*

We conjecture that Theorem 1 is best possible. Indeed, if p is prime and $2p^2 - 1$ is also prime, then for $n = p(2p^2 - 1)$, $\sigma(n)\phi(n) = (n - p)^2$ and $n \sim 2p^3$. It is conjectured that there are infinitely many such primes (this is a special case of Schinzel's Hypothesis H).

Next, we look at the set

$$\begin{aligned}\mathcal{A} &= \{a \geqslant 1 : \mathcal{N}_a \neq \emptyset\}\\ &= \{2, 3, 6, 7, 8, 9, 11, 13, 17, 19, 23, 24, 26, 28, 32, 35, 37, 40, 41, 43, 45, 47, 53, \ldots\}.\end{aligned}$$

Date: October 26, 2012.

[1]We use $\square$ to denote the square of a positive integer

Clearly, $\mathcal{A}$ is infinite because on the one hand there are infinitely many n such that $\phi(n)\sigma(n) = \square$, while on the other hand for each a the set $\mathcal{N}_a$ is finite by Theorem 1. Our next result gives a lower bound for $\mathcal{A}(x) = \mathcal{A} \cap [1, x]$.

thm:3 **Theorem 2.** *The estimate* $\#\mathcal{A}(x) \geqslant x^{1/8+o(1)}$ *holds as* $x \to \infty$.

In light of the examples given above ($n = p(2p^2 - 1)$) and the Bateman-Horn conjectures [4], it is likely that $\mathcal{A}(x) \gg x/\log^2 x$.

Throughout the paper, we use the Landau symbols O and o and the Vinogradov symbols $\gg$, $\ll$ and $\asymp$ with their usual meaning. We recall that $A = O(B)$, $A \ll B$ and $B \gg A$ are all equivalent and mean that the inequality $|A| \leqslant cB$ holds with some positive constant c. Further, $A \asymp B$ means that both estimates $A \ll B$ and $B \ll A$ hold, while $A = o(B)$ means that $A/B \to 0$. The symbols p, q always represent primes.

2 Background on solutions of Pell-type equations

Let $d > 1$ be a positive integer which is not a square. For $k \geqslant 1$, let (X_k, Y_k) be the kth positive solution of the Pell equation $X^2 - dY^2 = 1$. Recall that

$$X_k + \sqrt{d}Y_k = (X_1 + \sqrt{d}Y_1)^k \qquad \text{holds for all} \qquad k = 1, 2, \ldots$$

We shall use some basic facts about the sequences $(X_k)_{k\geqslant 1}$ such as relations of the type

$$X_{m+n} = X_m X_n + dY_m Y_n \qquad \text{for all positive integers} \qquad m,\ n,$$

as well as the fact that $X_m \mid X_n$ whenever $m \mid n$ and n/m is odd. We need the following easy result concerning the indices k such that X_k is an odd prime power.

lem:111 **Lemma 3.** *If* $X_k = p^\alpha$ *for some odd prime* p *and positive integer* α, *then* k *is a power of* 2.

Proof. Suppose that k is not a power of 2. Let $h \geqslant 3$ be an odd divisor of k and put $r = k/h$. Since $X_r \mid X_k$, we have $X_r = p^\beta$ for some integer $1 \leqslant \beta < \alpha$. From

$$X_k + \sqrt{d}Y_k = (X_r + \sqrt{d}Y_r)^h,$$

we get

eq:binom
$$X_k = \sum_{i=0}^{(h-1)/2} \binom{h}{2i+1} X_r^{2i+1}(X_r^2 - 1)^{(h-1)/2-i}. \tag{2.1}$$

In particular,

$$p^\alpha = X_k > X_r^h = (p^\beta)^h = p^{h\beta},$$

therefore $\beta < \alpha/h$. Let j be the largest integer with $p^{j\beta} \mid h$. If $j \leqslant h-2$, we then reduce the above equation (2.1) modulo $p^{(j+2)\beta}$. Upon observing that $j + 2 \leqslant h$, therefore $(j + 2)\beta \leqslant h\beta < \alpha$, we infer that $p^{(j+2)\beta} \mid X_k$. Thus,

eq:uwithb
$$0 \equiv \sum_{0\leqslant i\leqslant j/2} \binom{h}{2i+1} p^{(2i+1)\beta}(p^{2\beta} - 1)^{(h-1)/2-i} \pmod{p^{(j+2)\beta}}. \tag{2.2}$$

We now show that $p^{(j+2)\beta} \mid \binom{h}{2i+1} p^{(2i+1)\beta}$ for all $1 \leqslant i \leqslant j/2$. Indeed, let $p^\lambda \| 2i + 1$. Since $2i + 1 \leqslant p^{2i-1}$, it follows that $\lambda \leqslant 2i - 1$. Using Kummer's theorem concerning the power of a prime dividing a binomial coefficient and denoting by $\nu_p(m)$ the exponent of p in the factorization of m, we then have

$$\nu_p\left(\binom{h}{2i+1}\right) \geqslant \nu_p(h) - \nu_p(2i+1) \geqslant 2j\beta - \lambda,$$

so

$$(j+2)\beta \leqslant \nu_p\left(\binom{h}{2i+1}\right) + \lambda + 2\beta \leqslant \nu_p\left(\binom{h}{2i+1}\right) + (2i-1) + 2\beta \leqslant \nu_p\left(\binom{h}{2i+1}p^{(2i+1)\beta}\right).$$

Thus, $p^{(j+2)\beta} \mid \binom{h}{2i+1}p^{(2i+1)\beta}$. The congruence (2.2) then implies

$$0 \equiv hp^{\beta}(p^{2\beta}-1)^{(h-1)/2} \pmod{p^{(j+2)\beta}},$$

which implies $p^{(j+1)\beta} \mid h$, a contradiction. Hence, $j \geqslant h-1$, so h is divisible by $p^{h-1} > h$, a contradiction. $\square$

Let $a > 1$ and $b > 1$ be coprime square free integers such that the Diophantine equation

$$aU^2 - bV^2 = 1$$

has a positive integer solution (U, V). It is then well-known that it has infinitely many positive integer solutions (U, V). Further, putting (U_1, V_1) for the smallest such solution, all solutions of the above equation are of the form (U_{2j+1}, V_{2j+1}) for some $j \geqslant 0$, where

$$\sqrt{a}U_{2j+1} + \sqrt{b}V_{2j+1} = \gamma^{2j+1} \qquad \text{where} \qquad \gamma = \sqrt{a}U_1 + \sqrt{b}V_1.$$

Furthermore, if we put

$$\gamma^{2j} = U_{2j} + \sqrt{ab}V_{2j} \qquad \text{for} \qquad j \geqslant 1,$$

then the pairs $(X, Y) = (U_{2j}, V_{2j})$ for $j \geqslant 1$ form all the positive integer solutions of the Pell equation $X^2 - (ab)Y^2 = 1$. All these facts follow from Theorem 3 in [13]. We need the following result which is similar to Lemma 3.

lem:112 **Lemma 4.** *With the above notation, let $a = p$ be an odd prime and let h be an odd positive integer. If $U_h = p^{\alpha}$ for some $\alpha \geqslant 0$, then $h = 1$ or $(a, b, h) = (3, 2, 3)$.*

Proof. If $\alpha = 0$, then there is nothing to prove. So, assume that $\alpha > 0$ and $h > 1$. Write $h = rs$ with $1 \leqslant r < h$. Since $U_r \mid U_h$, it follows that $U_r = p^{\beta}$, where $0 \leqslant \beta < \alpha$. Write

binom2
$$p^{\alpha} = U_h = \sum_{i=0}^{(s-1)/2} \binom{s}{2i+1} U_r^{2i+1} p^i (bV_r^2)^{(s-1)/2-i}. \tag{2.3}$$

Let $p^j \| s$ and assume that $j < \alpha - \beta$. As in the previous proof, for $i \geqslant 1$ let $p^{\lambda} \| 2i+1$. Observe that $\lambda \leqslant i$ and in fact $\lambda \leqslant i-1$ except when $p = 3$ and $i = 1$. Then

$$\nu_p\left(\binom{s}{2i+1}\right) \geqslant \nu_p(s) - \nu_p(2i+1) = j - \lambda,$$

therefore

$$\nu_p\left(\binom{h}{2i+1}U_r^{2i+1}p^i\right) \geqslant j + (2i+1)\beta + i - \lambda.$$

If $\lambda \leqslant i-1$ or if $\beta > 0$, the right hand side above is at least $j+1+\beta$. Thus, in (2.3) all terms with $i \geqslant 1$ are divisible by $p^{j+1+\beta}$. This implies

$$0 \equiv sp^{\beta}(bV_1^2)^{(s-1)/2} \pmod{p^{j+1+\beta}},$$

so $p^{j+1} \mid s$, a contradiction. Thus, we have $j \geqslant \alpha - \beta$ and hence $U_h/U_r \mid s$. This is impossible, as (2.3) implies

$$\frac{U_h}{U_r} > p^{(s-1)/2} \geqslant s.$$

It remains to treat the exceptional case $i = 1, \beta = 0, p = 3$ for which $U_1 = 1, b = 2, V_1 = 1$. Note that in this case $U_3 = 9 = 3^2$. No other odd numbers h give $U_h = 3^\alpha$, however. To see this, apply (2.3) with $r = 1, s = h$ and deduce that $3|h$. If $h > 3$, we apply the above argument with $r = 3, s = h/3$ and $\beta = 2$, and deduce a contradiction as before. $\square$

The proofs of Lemma 3 and 4 can be simplified by invoking the Primitive Divisor Theorem for Lucas and Lehmer sequences (see [6], [15] and [5]). We gave the current proofs in order to make the proof of Theorem 1 self–contained.

3 The proof of Theorem 1

Suppose that $n \in \mathcal{N}_a$, let $k = \omega(n)$ and factor n canonically as $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. If $k = 1$, then $n = p_1^{\alpha_1}$ and

$$\phi(n)\sigma(n) = p_1^{\alpha_1 - 1}(p_1^{\alpha_1+1} - 1) = \square.$$

Since the two factors $p_1^{\alpha_1+1} - 1$ and $p_1^{\alpha_1-1}$ are coprime and their product is a square, it follows that each one of them is a square. So, $\alpha_1 - 1 = 2\beta_1$ is even, and $p_1^{\alpha_1+1} - 1 = p_1^{2\beta_1+2} - 1 = \square$, which is impossible because there are no two consecutive perfect squares. Hence, $k \geqslant 2$.

We apply the AGM–inequality to the right side of (1.2) and get

$$\begin{aligned}\left(1 - \frac{1}{k}\left(\sum_{i=1}^k \frac{1}{p_i^{\alpha_i+1}}\right)\right)^2 &\geqslant \left(1 - \frac{1}{k}\left(\sum_{i=1}^k \frac{1}{p_i^{\alpha_i+1}}\right)\right)^k \geqslant \prod_{i=1}^k \left(1 - \frac{1}{p_i^{\alpha_i+1}}\right) \\ &= \frac{\sigma(n)\phi(n)}{n^2} = \left(1 - \frac{a}{n}\right)^2.\end{aligned}$$

Taking square roots and rearranging gives

eq:4
$$ak \geqslant n\left(\sum_{i=1}^k \frac{1}{p_i^{\alpha_i+1}}\right). \tag{3.1}$$

Applying again the AGM–inequality to the right–hand side of (3.1), we get

$$ak \geqslant kn\prod_{i=1}^k p_i^{-(\alpha_i+1)/k} = k\prod_{i=1}^k p_i^{\alpha_i-(\alpha_i+1)/k}.$$

If $k \geqslant 3$, then since $\alpha_i - (\alpha_i+1)/k \geqslant \alpha_i - (\alpha_i+1)/3 = (2\alpha_i - 1)/3 \geqslant \alpha_i/3$ for all $i = 1, \ldots, k$, we get that

$$a \geqslant \prod_{i=1}^k p_i^{\alpha_i/3} = n^{1/3}.$$

Thus, if $k \geqslant 3$, then $n \leqslant a^3$.

Next, suppose $k = 2$ and rewrite equation (1.2) as

$$\prod_{i=1}^{2} p_i^{\alpha_i - 1}(p_i^{\alpha_i + 1} - 1) = (\prod_{i=1}^{2} p_i^{\alpha_i} - a)^2.$$

If $\alpha_i \geqslant 2$, then $p_i^{\alpha_i - 1} \mid a^2$, therefore $p_i \mid a$, and then $p_i^{\alpha_i} \mid a^3$. In particular, if $\alpha_1 > 1$ and $\alpha_2 > 1$, then $n = p_1^{\alpha_1} p_2^{\alpha_2} | a^3$, so that $n \leqslant a^3$. The next case is when $\alpha_1 = 1$ and $\alpha_2 \geqslant 2$. If $\alpha_2 = 2$, then $p_2 | a$, hence $p_1 < p_2 \leqslant a$ and $n = p_1 p_2^2 < a^3$. If $\alpha_2 \geqslant 3$, (3.1) implies that $2a \geqslant n/p_1^2 \geqslant p_2^{\alpha_2 - 1} \geqslant n^{1/2}$, so that $n \leqslant 4a^2 \leqslant 2a^3$ (recall that $a = 1$ is not possible).

The final case is when $k = 2$ and $\alpha_2 = 1$. Assume first that $p_1 = 2$. Then $p_2^2 - 1 \equiv 0 \pmod 8$, therefore $2^{\alpha_1 + 2} \mid \phi(n)\sigma(n) = (2^{\alpha_1} n - a)^2$, showing that $2^{\alpha_1 + 1} \mid a^2$. Thus, by equation (3.1), we get

$$n \leqslant 2^{\alpha_1 + 1}(2a) \leqslant 2a^3.$$

From now on, we suppose that p_1 is odd. We break the argument into two subcases depending on whether α_1 is odd or even. First, suppose α_1 is odd and write $\alpha_1 = 2\beta - 1$, where $\beta \geqslant 1$. Here we have $p_1^{\beta - 1} | a$, so we may write $a = p_1^{\beta - 1} b$ for a positive integer b. Then our equation becomes

$$(p_1^{2\beta} - 1)(p_2^2 - 1) = (p_1^{\beta} p_2 - b)^2.$$

Thus, there exists a square free number d and integers u, v such that $p_1^{2\beta} - 1 = du^2$ and $p_2^2 - 1 = dv^2$. Let (X_1, Y_1) be the minimal positive solution to the Pell equation $X^2 - dY^2 = 1$ and let (X_j, Y_j) be its jth solution. Since $p_1^{\beta} = X_\ell$ and $p_2 = X_m$ for some positive integers ℓ, m, it follows by Lemma 3 that both ℓ and m are powers of 2. Further, since

$$(X_\ell X_m - b)^2 = (p_1^{\beta} p_2 - a)^2 = (p_1^{2\beta} - 1)(p_2^2 - 1) = (dY_\ell Y_m)^2,$$

it follows that

$$b = X_\ell X_m - dY_\ell Y_m = X_{|m - \ell|}.$$

Suppose that $\beta \leqslant 2$. If $m < \ell$ then $p_1^{\beta} = X_\ell = 2X_{\ell/2}^2 - 1 \geqslant 2p_2^2 - 1 > p_2^2$, a contradiction. Hence, $m \geqslant 2\ell$ and $p_1^{\beta} = X_\ell \leqslant b$, which implies $a = p_1^{\beta - 1} b \geqslant p_1^{2\beta - 1}$. We also have $p_2 = X_m = 2X_{m/2}^2 - 1 < 2b^2 \leqslant 2a^2$ and consequently

$$n = p_1^{2\beta - 1} p_2 < 2a^3.$$

Now suppose $\beta \geqslant 3$. If $m \geqslant 2\ell$, then we get $b \geqslant X_k = p_1^{\beta}$ as before. Otherwise, $m \leqslant \ell/2$, $2|\ell$ and

$$b \geqslant X_{\ell/2} = \sqrt{\frac{X_\ell + 1}{2}} \geqslant \sqrt{\frac{p_1^{\beta}}{2}}.$$

In both cases,

$$a = p_1^{\beta - 1} b \leqslant \frac{p_1^{\beta - 1 + (\beta/2)}}{\sqrt{2}},$$

hence $p_1 \leqslant (a\sqrt{2})^{2/(3\beta - 2)}$. Using (3.1), we get $p_2 \leqslant 2ap_1 \leqslant 2a(a\sqrt{2})^{2/(3\beta - 2)}$ and we conclude that

$$n \leqslant 2a(a\sqrt{2})^{\frac{4\beta}{3\beta - 2}} = 2^{1 + \frac{2\beta}{3\beta - 2}} a^{\frac{7\beta - 2}{3\beta - 2}} < 4a^{19/7} \leqslant 2a^3,$$

the final inequality holding for $a \geqslant 12$ (for $a \leqslant 11$, a quick search yields no solutions in the interval $[2a^3, 4a^{19/7}]$). This concludes the proof when α_1 is odd.

Finally, suppose α_1 is even and write $\alpha_1 = 2\beta$. Then $p_1^{\beta} \mid a$ and $p_1 \mid p_2^2 - 1$. Writing $a = p_1^{\beta} a_1$, we get

$$(p_1^{2\beta + 1} - 1)\left(\frac{p_2^2 - 1}{p_1}\right) = (p_1^{\beta} p_2 - a_1)^2.$$

In particular, there exists a square free number d and integers u and v such that

$$p_1^{2\beta+1} - 1 = du^2 \quad \text{and} \quad p_2^2 - 1 = p_1 dv^2.$$

If $d = 1$, then the first equation above becomes $p_1^{2\beta+1} - u^2 = 1$, which has no solutions by known results on Catalan's equation (this particular case of Catalan's equation was solved by Lebesque in [12] more than 160 years ago). Thus, $d > 1$. Putting $x = p_1^\beta$ and $y = p_2$, we get

$$\begin{aligned} p_1 x^2 - du^2 &= 1; \\ y^2 - (p_1 d)v^2 &= 1. \end{aligned}$$

With the notation from the previous section, let $\gamma = U_1\sqrt{p_1} + V_1\sqrt{d}$ and $\delta = U_1\sqrt{p_1} - V_1\sqrt{d}$. Then

$$p_1^\beta = U_\ell \qquad \text{and} \qquad p_2 = U_m$$

for some positive integers ℓ odd and m even. By Lemma 4, we have $\ell = 1$ or $(p, x) = (3, 9)$. In the latter case, using (3.1) gives $n = 3^4 p_2 \leqslant 3^4(6a) \leqslant 2a^3$ for $a \geqslant 16$ (for $a \leqslant 15$, there are no solutions $n \in [2a^3, 486a]$). Now suppose $\ell = 1$. By Lemma 3, m is a power of 2 and we get

$$\begin{aligned} a_1 = p_1^\beta p_2 - duv &= \left(\frac{\gamma+\delta}{2\sqrt{p_1}}\right)\left(\frac{\gamma^m+\delta^m}{2}\right) - \left(\frac{\gamma-\delta}{2}\right)\left(\frac{\gamma^m-\delta^m}{2\sqrt{p_1}}\right) = \frac{\gamma^{m-1}+\delta^{m-1}}{2\sqrt{p_1}} \\ &= U_{m-1} \geqslant U_1 = p_1^\beta. \end{aligned}$$

Hence, $a \geqslant p_1^{2\beta}$ and we conclude that

$$n = p_1^{2\beta} p_2 \leqslant ap_2 \leqslant a(2ap_1) \leqslant 2a^{2+1/(2\beta)} \leqslant 2a^{5/2}.$$

4 The proof of Theorem 2

4.1 Preliminary results

For an integer m we use $P(m)$ for the largest prime factor of m with the convention that $P(0) = P(\pm 1) = 1$. If m satisfies $P(m) \leqslant y$, then m is called y–smooth.

We follow [11]. Given a polynomial $F(X) \in \mathbb{Z}[X]$ put

$$\pi_F(x, y) = \#\{p \leqslant x : P(F(p)) \leqslant y\}.$$

The following result appears in [9].

lem:11 **Lemma 5.** *Let g be the largest of the degrees of the irreducible factors of $F(X)$ and let k be the number of irreducible factors of $F(X)$ of degree g. Assume that $F(0) \neq 0$ if $g = k = 1$, and let ε be any positive number. Then the estimate*

$$\pi_F(x, y) \asymp \frac{x}{\log x}$$

holds for all sufficiently large x provided that $y \geqslant x^{g+\varepsilon-1/2k}$.

In the remaining of this section, G is a finite abelian group. Let $n(G)$ be length of the longest sequence of elements of G (not necessarily distinct) such that no nonempty subsequence of it has a zero sum. The following result is from [10].

lem:12 **Lemma 6.** *If m is the maximal order of an element of G, then*

$$n(G) < m(1 + \log(\#G/m)).$$

The following result is from [1].

lem:13 **Lemma 7.** *Assume that $r > k > n = n(G)$ be integers. Then any sequence of r elements of G contains at least $\binom{r}{k}/\binom{r}{n}$ distinct subsequences of length between $k-n$ and k having zero sum.*

4.2 The proof of Theorem 2

Let x be large, $\varepsilon \in (0, 1/5)$, $x_1 = x^{1/2-\varepsilon}$ and

$$y = \frac{\log x_1}{\log\log x_1}.$$

Let $t = \pi(y)$ and $G = (\mathbb{Z}/2\mathbb{Z})^t$, so by Lemma 6,

eq:nG
$$n(G) < 2(1 + (\pi(y) - 1)\log 2). \tag{4.1}$$

Let $u = (3/4 + \varepsilon)^{-1}$. Applying Lemma 5 to the polynomial $F(X) = X^2 - 1$ for which $g = 1$ and $k = 2$, we get that

$$\pi_F(y^u, y) \gg \frac{y^u}{\log y^u}.$$

In particular, by the Prime Number Theorem, there exists $c_1 \in (0, 1)$ such that if we put

eq:S1
$$\begin{aligned} \mathcal{S}_1(y) = \{p : c_1 y^u < p \leqslant y^u,\ P(p^2-1) \leqslant y\}, \qquad & \text{then} \\ \#\mathcal{S}_1(y) \gg \frac{y^u}{\log y^u}, \qquad \text{for} \qquad x > x_0. & \qquad (4.2) \end{aligned}$$

Applying the above argument with with y replaced by $c_1 y$, we also get that that if we put

eq:S2
$$\begin{aligned} \mathcal{S}_2(y) &= S_1(c_1 y) = \{p : c_1^{u+1} y^u < p \leqslant c_1^u y^u,\ P(p^2-1) \leqslant c_1 y\}, \quad \text{then} \\ \#\mathcal{S}_2(y) &\gg \frac{(c_1 y)^u}{\log((c_1 y)^u)} \gg \frac{y^u}{\log y^u}, \qquad \text{for} \qquad x > x_0. \qquad (4.3) \end{aligned}$$

We put

$$k = \left\lfloor \frac{\log x_1}{\log y^u} \right\rfloor.$$

The argument from the proof of Theorem 1.1 in [11] shows that if we put

$$\mathcal{F}(y) = \{\ell < x_1 : \phi(\ell)\sigma(\ell) = \square \text{ and } p \in \mathcal{S}_1(y) \text{ for all } p \mid \ell\},$$

then

$$T = \#\mathcal{F}(y) = x_1^{1-1/u+o(1)} > x^{1/8-\varepsilon}$$

for large x. Now take

eq:M
$$M = \left\lfloor \frac{\log x_1}{\log(c_1^{u+1} y^u)} \right\rfloor + n(G) + 2. \tag{4.4}$$

Note that

$$M \ll \frac{\log x_1}{\log y} + 2\pi(y) \ll y,$$

so in particular $2M < \#\mathcal{S}_2(y)$ for large x by inequality (4.3). Choose elements $q_1, \ldots, q_{2M}$ in $\mathcal{S}_2(y)$ and write $q_i^2 - 1 = a_i\square$, where a_i is square free and $P(a_i) \leqslant y$ for $i = 1, \ldots, 2M$. We think of a_i as elements G where in the location corresponding to a prime $p \leqslant y$ we assign the value 1 or 0 according to whether p divides a_i or not. We apply Lemma 7 with $r = 2M,\ k = M$ to deduce the existence of at least $\binom{2M}{M}/\binom{2M}{n(G)} > 1$ subsequences of length at most M and at least $M - n(G)$ with a zero sum. Fix one such subsequence $\{q_i\}_{i\in I}$ and put

$$w = \prod_{i\in I} q_i.$$

Then $\phi(w)\sigma(w) = v^2$ for some integer v. Furthermore, since

$$\left\lfloor \frac{\log x_1}{\log(c_1^{u+1}y^u)} \right\rfloor + 2 \leqslant \#I \leqslant M \leqslant \left\lfloor \frac{\log x_1}{\log(c_1^{u+1}y^u)} \right\rfloor + n(G) + 2,$$

we get that

eq:large

$$w \geqslant (c_1^{u+1}y^u)^{\#I} \geqslant (c_1^{u+1}y^u)^{\left\lfloor \frac{\log x_1}{\log(c_1^{u+1}y^u)} \right\rfloor + 2} > 2x_1 > 2\ell \tag{4.5}$$

for all $\ell \in \mathcal{F}(y)$ when $x > x_0$, and

$$w < (c_1^{u}y^u)^{\left\lfloor \frac{\log x_1}{\log(c_1^{u+1}y^u)} \right\rfloor + O(\pi(y))} = x_1^{1+o(1)} < x^{1/2+\varepsilon}$$

for all sufficiently large x, where we used the fact that (see (4.1)),

$$n(G) \ll \pi(y) = o(y) = o\left(\frac{\log x}{\log(c_1^{u+1}y^u)}\right) \qquad (x \to \infty).$$

Now consider

$$\mathcal{N}(y) = \{w\ell : \ell \in \mathcal{F}(y)\}.$$

Clearly, $n < x_1 w < x$ for all $n \in \mathcal{N}(y)$. Let $\ell_1, \ldots, \ell_T$ be all the elements of $\mathcal{F}(y)$. Let $n_i = \ell_i w$ for $i = 1, \ldots, T$. Then

$$\sigma(n_i)\phi(n_i) = (n_i - a_i)^2.$$

Clearly, $a_i < n_i < x$. Let us show that these a_i's are distinct. Put $\phi(n_i)\sigma(n_i) = m_i^2$ for $i = 1, \ldots, T$. If $a_i = a_j (= a)$ for some $i \neq j$, then

$$m_i = n_i - a \quad \text{and} \quad m_j = n_j - a,$$

so

eq:t

$$m_i - m_j = n_i - n_j = (\ell_i - \ell_j)w. \tag{4.6}$$

Observe that w is built with primes $p \leqslant c_1^u y^u < c_1 y^u$ and the numbers ℓ_s are built with primes $p > c_1 y^u$ for $s = 1, 2, \ldots, T$, so $\gcd(\ell_s, w) = 1$. Hence, m_s is a multiple of v for all $s = 1, \ldots, T$. Thus, the left-hand side in (4.6) is a multiple of v. Clearly,

$$v = \sqrt{\phi(w)\sigma(w)} = w \prod_{q|w}\left(1 - \frac{1}{q^2}\right)^{1/2} > \frac{w}{\sqrt{\zeta(2)}} > \frac{w}{2} > \max\{\ell_i, \ell_j\} > |\ell_i - \ell_j|,$$

by inequality (4.5). Furthermore, v is divisible only by primes $p < y$, whereas w is divisible only by primes $q > c_1^{u+1}y^u > y$ for x sufficiently large, so that $\gcd(v, w) = 1$. Now equation (4.6) implies that $v|(\ell_i - \ell_j)$, hence $\ell_i = \ell_j$. So, $a_1, \ldots, a_T$ are distinct, therefore

$$\#\mathcal{A}(x) \geqslant T = \#\mathcal{F}(y) \geqslant x^{1/8-\varepsilon+o(1)}$$

as $x \to \infty$. Letting ε tend to zero, we obtain the desired estimate.

Remarks. If, as widely believed, for any $\varepsilon > 0$ we have $\pi_F(x, x^\varepsilon) \gg x/\log x$, then the above argument implies that $\#\mathcal{A}(x) > x^{1/2-o(1)}$ as $x \to \infty$.

Acknowledgements

F. L. worked on this paper during a visit to the Faculty of Computing and Mathematical Sciences of the University of Waikato in Hamilton, New Zealand in December of 2011 and during a visit to the University of Illinois in Urbana Champaign in March of 2012, while K. F. worked on this paper during a visit to the Mathematical Institute of the UNAM in Morelia, Mexico in December of 2011. They thank the people of the corresponding institutions for their hospitality. K. F. was supported in part by National Science Foundation grant DMS-0901339. F. L. was supported in part by Project PAPIIT IN104512 and a Marcos Moshinsky Fellowship.

References

agp [1] W. R. Alford, A. Granville and C. Pomerance, “There are infinitely many Carmichael numbers”, *Ann. Math. (2)* **139** (1994), 703–722.

apostol [2] T. M. Apostol, *Introduction to analytic number theory*, Springer, 1976.

banks [3] W. D. Banks, J. B. Friedlander, C. Pomerance and I. E. Shparlinski, “Multiplicative structure of values of the Euler function”, *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, Fields Inst. Commun., **41**, Amer. Math. Soc, (2004), 29–47.

BT [4] P. T. Bateman and R. A. Horn, “A heuristic asymptotic formula con- cerning the distribution of prime numbers”, *Math. Comp.* **16** (1962), 363–367.

BHV [5] Yu. F. Bilu, G. Hanrot and P. M. Voutier, “Existence of primitive divisors of Lucas and Lehmer numbers. With an appendix by M. Mignotte”, *J. reine angew Math.* **539** (2001), 75–122.

Car [6] R. D. Carmichael, “On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$”, *Ann. Math. (2)* **15** (1913), 30–70.

CEP [7] E. R. Canfield, P. Erdős and C. Pomerance, “On a problem of Oppenheim concerning ”factorisatio numerorum”,” *J. Number Theory* **17** (1983), 1–28.

Cohn [8] J. H. E. Cohn, “The Diophantine equation $x^4 - Dy^2 = 1$. II”, *Acta Arith.* **78** (1997), 401–403.

DMT [9] C. Dartyge, G. Martin and G. Tenenbaum, “Polynomial values free of large prime factors”, *Per. Math. Hungarica* **43** (2001), 111–119.

boas [10] P. van Emde Boas and D. Kruyswijk, “A combinatorial problem on finite abelian groups III”, *Math. Centrum Amsterdam, Adf. Zuivere Wisk. ZW* 1969–008, 1969.

Frei [11] T. Freiberg, “Products of shifted primes simultaneously taking perfect power values”, (preprint).

Le [12] V. A. Lebesgue, “Sur limpossibilité en nombres entiers de lequation $x^m = y^2 + 1$”, *Nouvelle Annales des Mathématiques (1)* **9** (1850), 178–181.

Nagell [13] T. Nagell, “On a special class of Diophantine equations of the second degree”, *Ark. Mat.* **3** (1954), 51–65.

Hand [14] J. Sándor, D. S. Mitrinović, B. Crstici, *Handbook of number theory. I.* Second printing of the 1996 original. Springer, Dordrecht, 2006.

War [15] M. Ward, “The intrinsic divisors of Lehmer numbers”, *Ann. Math. (2)* **62** (1955), 230–236.

Department of Mathematics, University of Waikato, Private Bag 3105, Hamilton, New Zealand.

E-mail address: kab@waikato.ac.nz

Department of Mathematics, The University of Illinois at Urbana-Champaign Urbana, 1409 West Green St., Champaign, IL 61801, USA.

E-mail address: ford@math.uiuc.edu

Centro de Ciencias Matemáticas, Universidad Nacional Autonoma de México, C.P. 58089, Morelia, Michoacán, México.

E-mail address: fluca@matmor.unam.mx