Glasgow Math. J. **51** (2009) 83–89.
doi:10.1017/S0017089508004552. Printed in the United Kingdom

A VARIANT ON THE NOTION OF A DIOPHANTINE s-TUPLE

WILLIAM D. BANKS†

Department of Mathematics University of Missouri Columbia, MO 65211 USA
e-mail: bbanks@math.missouri.edu

FLORIAN LUCA

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

and LÁSZLÓ SZALAY

Institute of Mathematics and Statistics University of West Hungary H-9400 Sopron, Erzsébet u. 9, Hungary
e-mail: laszalay@ktk.nyme.hu

(Received 26 December 2007; accepted 15 July 2008)

Abstract. We show that there is an infinite set $\mathcal{S}$ of natural numbers with the property that $1 + \prod_{n\in\mathcal{R}} n$ is square-free for every finite subset $\mathcal{R} \subseteq \mathcal{S}$.

2000 *Mathematics Subject Classification.* MSC Numbers: 11B99, 11N25.

1. Introduction.

1.1. Diophantine s-tuples. In the third century, Diophantus of Alexandria studied sets $\mathcal{S}$ of positive rational numbers with the property that $1 + mn$ is the square of a rational number for all $m, n \in \mathcal{S}$, $m \neq n$. One example he found was the set

$$\mathcal{S}_d = \left\{ \frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16} \right\}.$$

In the 17th century, Fermat considered Diophantus' problem, but he was mainly interested in sets that contain only natural numbers. A set of this type is called a *Diophantine s-tuple* if it has s elements. Fermat found the first Diophantine quadruple:

$$\mathcal{S}_f = \{1, 3, 8, 120\}.$$

Euler showed that Fermat's set can be extended to a larger set of *rational numbers* with Diophantus' property, namely,

$$\mathcal{S}_e = \left\{ 1, 3, 8, 120, \frac{777480}{8288641} \right\}.$$

On the other hand, Baker and Davenport [**1**] showed that Fermat's set $\mathcal{S}_f$ cannot be extended to include a fifth *natural number*. Dujella [**3**] has shown that there are no

†Corresponding author

Diophantine sextuples and that there are at most finitely many Diophantine quintuples; it is unknown whether any such quintuples exist.

1.2. Generalizations.

The notion of a Diophantine s-tuple is easily generalized by replacing the set of square numbers with an arbitrary set of natural numbers.

DEFINITION 1. For a given set $\mathcal{A} \subseteq \mathbb{N}$, we say that $\mathcal{S} \subseteq \mathbb{N}$ is *$\mathcal{A}$-Diophantine* if $1 + mn \in \mathcal{A}$ for all $m, n \in \mathcal{S}$, $m \neq n$.

With this terminology, a Diophantine s-tuple is simply an $\mathbb{N}^2$-Diophantine set with s elements, where $\mathbb{N}^2$ is the set of square numbers. The result of Dujella asserts that $\#\mathcal{S} \leqslant 5$ for every $\mathbb{N}^2$-Diophantine set $\mathcal{S}$ and $\#\mathcal{S} = 5$ holds for at most finitely many such sets $\mathcal{S}$.

One can also consider the following stronger condition on a set $\mathcal{S} \subseteq \mathbb{N}$:

DEFINITION 2. Given $\mathcal{A} \subseteq \mathbb{N}$, we say that $\mathcal{S} \subseteq \mathbb{N}$ is *strongly $\mathcal{A}$-Diophantine* if $1 + \prod_{n \in \mathcal{R}} n \in \mathcal{A}$ for every finite subset $\mathcal{R} \subseteq \mathcal{S}$.

It is easy to check that the set

$$\mathcal{S}_p = \{2, 3, 6, 26, 90, 336, 476, 3926\}$$

has the property that $1 + mn$ is a prime number for all $m, n \in \mathcal{S}_p$, $m \neq n$. In other words, $\mathcal{S}_p$ is $\mathcal{P}$-Diophantine, where $\mathcal{P}$ is the set of prime numbers. The set $\mathcal{S}_p$ is not strongly $\mathcal{P}$-Diophantine, but such sets do exist and are easily found by computer (e.g., $\mathcal{S}_p^* = \{1, 2, 6, 96\}$). It is natural to ask whether there exists a $\mathcal{P}$-Diophantine set with infinitely many elements, and we conjecture that this is the case. In Section 3, we show that a well-known and widely believed conjecture of Dickson implies the existence of a strongly $\mathcal{P}$-Diophantine set of infinite cardinality.

1.3. Statement of the main result.

In this note, we focus on a variant of Diophantus' problem with square-free numbers rather than square numbers. Our aim is to prove the existence of a strongly $\mathcal{A}$-Diophantine set of infinite cardinality, where $\mathcal{A}$ is the set of square-free natural numbers.

THEOREM 1. *There is an infinite set $\mathcal{S} \subseteq \mathbb{N}$ with the property that $1 + \prod_{n \in \mathcal{R}} n$ is square-free for every finite subset $\mathcal{R} \subseteq \mathcal{S}$. Moreover, for $x \geqslant 3$, we have*

$$\#\{n \leqslant x \; : \; n \in \mathcal{S}\} \gg \sqrt{\log \log x}. \tag{1}$$

2. Construction.

In what follows, the letter p always denotes a prime number. For a positive integer, $\omega(n)$ denotes the number of distinct prime divisors of n. For positive functions f and g, the notation $f \ll g$ means that the inequality $f \leqslant cg$ holds with some absolute constant $c > 0$.

Our principal tool is the following technical lemma, which is a consequence of the more general result (Lemma 2) of Luca and Shparlinski [**4**]:

LEMMA 1. *For any real number $y \geqslant 2$, let $K = \prod_{p \leqslant y} p$. Let $\{A_1, \dots, A_s\}$ be a set of positive integers with the property that the products*

$$P_{\mathcal{T}} = \prod_{j \in \mathcal{T}} A_j \qquad (\mathcal{T} \subseteq \mathcal{U} = \{1, \dots, s\})$$

are pairwise distinct and put

$$F(X) = \prod_{\mathcal{T} \subseteq \{1, \dots, s\}} (P_{\mathcal{T}} K X + 1) \in \mathbb{Z}[X].$$

Finally, let Δ be the product of the distinct primes $p > y$ that divide the product

$$\prod_{\substack{\mathcal{T}_1, \mathcal{T}_2 \subseteq \{1, \dots, s\} \\ \mathcal{T}_1 \neq \mathcal{T}_2}} |P_{\mathcal{T}_1} - P_{\mathcal{T}_2}|. \tag{2}$$

Then,

$$\#\{n \leqslant x \ : \ F(n) \text{ is square-free}\} \geqslant x \left(1 - \frac{2^s}{y}\right)^{\omega(\Delta)} - 2^{s\,\omega(\Delta)} - \frac{2^s x}{y} - 2^s \sqrt{Mx},$$

where $M = 1 + P_{\mathcal{U}} K$.

Proof of Theorem 1. For every real number t, we write $\exp_2(t) = \exp(e^t)$, and we put

$$f(t) = \exp_2(16t^2) \qquad \text{and} \qquad g(t) = \log f(t + 1/4) = e^{16t^2 + 8t + 1}. \tag{3}$$

To prove the theorem, we construct an infinite sequence $A_1, A_2, A_3, \dots$ of distinct positive integers such that for every integer $s \geqslant 1$ the following properties hold:

(i) the products $P_{\mathcal{T}} = \prod_{j \in \mathcal{T}} A_j$ with $\mathcal{T} \subseteq \{1, \dots, s\}$ are pairwise distinct;
(ii) the bound $A_j \leqslant f(j)$ holds for each $j = 1, \dots, s$;
(iii) the number $1 + P_{\mathcal{T}}$ is square-free for every subset $\mathcal{T} \subseteq \{1, \dots, s\}$.

Assuming this has been done, we put $\mathcal{S} = \{A_j \ : \ j \geqslant 1\}$. Then, for every finite subset $\mathcal{R} \subseteq \mathcal{S}$, we have $1 + \prod_{n \in \mathcal{R}} n = 1 + P_{\mathcal{T}}$, where $\mathcal{T} = \{j \ : \ A_j \in \mathcal{R}\}$; hence, this number is square-free. As the construction in the following text produces a set $\mathcal{S}$ with $A_1 = 2$, it suffices to establish the lower bound (1) for all sufficiently large values of x. For such x, we let s be determined by the inequalities

$$f(s) = \exp_2(16s^2) < x \leqslant \exp_2(16(s+1)^2).$$

Then,

$$\#\{n \leqslant x \ : \ n \in \mathcal{S}\} \geqslant \#\{A_1, \dots, A_s\} = s \gg \sqrt{\log \log x}$$

as required.

Turning now to our construction, let $A_1 = 2$, and note that (i) – (iii) hold with $s = 1$. Proceeding by induction, we suppose that $A_1, \dots, A_s$ have been defined and satisfy (i) – (iii) for some integer $s \geqslant 1$. We find a new integer $A_{s+1} \neq A_j$ for $j = 1, \dots, s$ such that the longer sequence $A_1, \dots, A_{s+1}$ satisfies:

https://doi.org/10.1017/S0017089508004552 Published online by Cambridge University Press

(*iv*) the products $P_{\mathcal{T}'} = \prod_{j\in\mathcal{T}'} A_j$ with $\mathcal{T}' \subseteq \{1, \ldots, s+1\}$ are pairwise distinct;
(*v*) the bound $A_j \leqslant f(j)$ holds for each $j = 1, \ldots, s+1$;
(*vi*) the number $1 + P_{\mathcal{T}'}$ is square-free for every subset $\mathcal{T}' \subseteq \{1, \ldots, s+1\}$.

To this end, we now define

$$y = g(s) \qquad \text{and} \qquad K = \prod_{p\leqslant y} p.$$

Using the upper bound $K \leqslant e^{2y}$ (see [**5**, Chapter I.1.2, Theorem 4]), we have

$$K \leqslant e^{2g(s)}. \tag{4}$$

From (*ii*), we derive the bound

$$P_{\mathcal{S}} = \prod_{j=1}^{s} A_j \leqslant f(s)^s.$$

Put $M = 1 + P_{\mathcal{S}}K$. Using the previous bound together with (4), we see that

$$M \leqslant 2P_{\mathcal{S}}K \leqslant 2f(s)^s e^{2g(s)}. \tag{5}$$

Now let Δ be the product of the distinct primes $p > y$ that divide the product (2). Since

$$\left|P_{\mathcal{T}_1} - P_{\mathcal{T}_2}\right| < P_{\mathcal{S}} \leqslant f(s)^s$$

for each factor in (2), we have the crude bound

$$\Delta \leqslant P_{\mathcal{S}}^{2^{s+1}} \leqslant f(s)^{s2^{s+1}}.$$

As Δ is composed of primes exceeding y, it follows that

$$\omega(\Delta) \leqslant \frac{\log \Delta}{\log y} \leqslant \frac{s2^{s+1}\log f(s)}{\log g(s)}. \tag{6}$$

Let

$$F(X) = \prod_{\mathcal{T}\subseteq\{1,\ldots,s\}} (P_{\mathcal{T}}KX + 1) \in \mathbb{Z}[X].$$

Using Lemma 1 with $x = f(s+1/4)^4 = e^{4g(s)}$ together with the bounds (5) and (6), we deduce that

$$\#\{n \leqslant e^{4g(s)} \ : \ F(n) \text{ is square-free}\} \geqslant L_1 - L_2 - L_3 - L_4, \tag{7}$$

where

$$L_1 = e^{4g(s)}\left(1 - \frac{2^s}{g(s)}\right)^{s2^{s+1}\log f(s)/\log g(s)};$$
$$L_2 = 2^{s^2 2^{s+1}\log f(s)/\log g(s)};$$

https://doi.org/10.1017/S0017089508004552 Published online by Cambridge University Press

$$L_3 = \frac{2^s e^{4g(s)}}{g(s)};$$
$$L_4 = 2^s \sqrt{2f(s)^s e^{6g(s)}}.$$

Since $\log(1-t) \geqslant -2t$, if $0 \leqslant t \leqslant 1/2$, and $g(s) = e^{16s^2+8s+1} \geqslant 2^{s+1}$, we have

$$\log\left(\frac{L_1}{e^{4g(s)}}\right) = \frac{s2^{s+1}\log f(s)}{\log g(s)} \log\left(1 - \frac{2^s}{g(s)}\right) \geqslant -\frac{s2^{2s+2}\log f(s)}{g(s)\log g(s)}. \tag{8}$$

In view of the definitions (3), it follows that

$$\frac{s2^{2s+2}\log f(s)}{g(s)\log g(s)} = \frac{s2^{2s+2}}{(16s^2+8s+1)e^{8s+1}} \leqslant 10^{-4}.$$

Combining this bound with (8), we deduce that

$$L_1 \geqslant 0.8\, e^{4g(s)}. \tag{9}$$

Similarly, we have

$$\log L_2 \leqslant \frac{s^2 2^{s+1}\log f(s)}{\log g(s)} \leqslant 10^{-4} \leqslant 4g(s) - \log 5$$

and therefore

$$L_2 \leqslant 0.2\, e^{4g(s)}. \tag{10}$$

Since $g(s) \geqslant 5 \cdot 2^s$, we also have

$$L_3 \leqslant 0.2\, e^{4g(s)}. \tag{11}$$

Finally, by the definitions (3), we see that

$$\log L_4 \leqslant s + 1 + 0.5s\log f(s) + 3g(s) \leqslant 4g(s) - \log 5$$

since

$$e^{16s^2+8s+1} \geqslant s + 1 + 0.5se^{16s^2} + \log 5;$$

therefore,

$$L_4 \leqslant 0.2\, e^{4g(s)}. \tag{12}$$

Now, inserting the estimates (9)–(12) into (17), it follows that

$$\#\{n \leqslant e^{4g(s)} \;:\; F(n) \text{ is square-free}\} \geqslant 0.2\, e^{4g(s)} \geqslant 2^{2s} + 1.$$

Hence, there is a positive integer $n \leqslant e^{4g(s)}$ such that $F(n)$ is square-free, and

$$nK \neq \frac{P_{\mathcal{T}_1}}{P_{\mathcal{T}_2}} \qquad \text{for all subsets } \mathcal{T}_1, \mathcal{T}_2 \text{ of } \{1, \ldots, s\}. \tag{13}$$

https://doi.org/10.1017/S0017089508004552 Published online by Cambridge University Press

Put $A_{s+1} = nK$ for any such n and note that

$$A_{s+1} \neq A_j = \frac{P_{\{j\}}}{P_{\varnothing}} \qquad (j = 1, \ldots, s).$$

It remains to show that the sequence $A_1, \ldots, A_{s+1}$ satisfies $(iv) - (vi)$. Since the products $P_{\mathcal{T}'} = \prod_{j \in \mathcal{T}'} A_j$ with $\mathcal{T}' \subseteq \{1, \ldots, s+1\}$ all have the form $P_{\mathcal{T}}$ or $P_{\mathcal{T}} A_{s+1}$ for a subset $\mathcal{T} \subseteq \{1, \ldots, s\}$, namely, $\mathcal{T} = \mathcal{T}' \setminus \{s+1\}$, the property (iv) is an immediate consequence of (i) and (13). Taking (ii) into account, property (v) is a consequence of the following bound:

$$A_{s+1} = nK \leqslant e^{4g(s)} e^{2g(s)} = \exp\left(6\, e^{16s^2+8s+1}\right) \leqslant \exp\left(e^{16s^2+32s+16}\right) = f(s+1).$$

Finally, property (vi) follows from (iii) and the fact that for every subset $\mathcal{T} \subseteq \{1, \ldots, s\}$, the number $1 + P_{\mathcal{T}} A_{s+1} = 1 + P_{\mathcal{T}} Kn$ is square-free since it divides the square-free number $F(n)$. □

3. Remarks. Let $\mathcal{A}$ be the set of square-free natural numbers and let $\mathcal{S}$ be strongly $\mathcal{A}$-Diophantine as in Theorem 1. It would be interesting either to improve the lower bound (1) on $\#(\mathcal{S} \cap [1, x])$ or to find a construction of such a set that yields a somewhat comparable upper bound for this quantity.

Suppose that $A_1 < \cdots < A_s$ are the first s elements in a strongly $\mathcal{A}$-Diophantine set $\mathcal{S}$. For a fixed subset $\mathcal{R} \subseteq \{1, \ldots, s\}$, the expectation that a random integer n has the property that $n \prod_{j \in \mathcal{R}} A_j + 1$ is square-free is $c_{\mathcal{R}} \cdot 6/\pi^2 \geqslant 6/\pi^2$, where $c_{\mathcal{R}} = \prod_{p \mid \prod_{j \in \mathcal{R}} A_j} (1 - p^{-2})^{-2}$. If we assume that these events are independent as $\mathcal{R}$ varies, then the probability that these numbers are simultaneously square-free for all subsets $\mathcal{R} \subseteq \{1, \ldots, s\}$ exceeds $(6/\pi^2)^{2^s}$. Therefore, writing $x = (s+1)(\pi^2/6)^{2^s}$, it is reasonable to expect that the interval $[1, x]$ contains at least $s + 1$ numbers n with this property if s is large; in particular, at least one of them is not in the set $\{A_1, \ldots, A_s\}$. Since $s \sim c \log\log x$, where $c = 1/\log 2$, this heuristic argument suggests that there exists a strongly $\mathcal{A}$-Diophantine set $\mathcal{S}$ for which $\#(\mathcal{S} \cap [1, x]) \asymp \log\log x$ as $x \to \infty$.

Here we give some numerical examples. The finite set

$$\mathcal{S} = \{1, 2, 5, 6, 9, 21, 42, 101, 330, 5738, 71190, 206083605\}$$

is strongly $\mathcal{A}$-Diophantine. Based on the heuristic argument, we expect that the next integer that can be added to this set, assuming it exists, must be quite large (if $A_1 < A_2 < \cdots$ are the elements of $\mathcal{S}$, then the number of digits in the decimal representation of A_j should grow as an exponential function of j). The set

$$\mathcal{S} = \{1, 2, 5, 6, 9, 10, 14, 18, 21, 30, 33, 42, 45, 50, 64, 65, 77, 81, 82, 92, 100\}$$

is $\mathcal{A}$-Diophantine (but not strongly so). This set was produced by using a greedy algorithm and can be extended to include 1,229 numbers below 10^8.

Let $\mathcal{B}$ be the set of natural numbers that are *not* square-free. Terr **[6]** has shown that for any integer k, there exists an infinite set $\mathcal{S}$ such that $k + mn \in \mathcal{B}$ for all $m, n \in \mathcal{S}$, $m \neq n$. In particular, there exists a $\mathcal{B}$-Diophantine set with infinitely many elements.

Since the set $\mathcal{P}$ of prime numbers is contained in the set $\mathcal{A}$ of square-free numbers, in view of Theorem 1 it is natural to ask whether there exists a $\mathcal{P}$-Diophantine set with infinitely many elements. We expect that the answer to this question is yes, but we do not know how to approach it. If the first s elements $A_1 < \cdots < A_s$ in $\mathcal{S}$ have already been constructed, then the collection of linear polynomials

$$f_{\mathcal{R}}(X) = X \prod_{j \in \mathcal{R}} A_j + 1 \qquad (\varnothing \neq \mathcal{R} \subseteq \{1, \ldots, s\})$$

satisfies the hypothesis of Dickson's generalized twin prime conjecture (see [**2**]); that is, for every prime p there is an integer n such that $p \nmid f_{\mathcal{R}}(n)$ for every $\mathcal{R}$ (indeed, one can take any n that is divisible by p). Then, Dickson's conjecture asserts that there is an integer $A_{s+1} > A_s$ such that $f_{\mathcal{R}}(A_{s+1})$ is prime for every $\mathcal{R}$ and this integer can be incorporated into the set $\mathcal{S}$.

ACKNOWLEDGEMENTS. We thank the referee for useful comments on the original manuscript. This work began during a mutual visit by the authors to the University of West Georgia for the INTEGERS Conference 2007 and continued during a subsequent visit by the third author to the University of Missouri; the support and kind hospitality of these institutions are gratefully acknowledged. During the preparation of this paper, F.L. was supported in part by Grants SEP-CONACyT 46755 and PAPIIT IN100508 and L.S. was supported in part by a János Bolyai scholarship of HAS and the Hungarian National Foundation for Scientific Research grant nos. T 048945 MAT and K 61800 FT2.

REFERENCES

1. A. Baker and H. Davenport, The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$, *Quart. J. Math. Oxford Ser.* **20**(2) (1969), 129–137.

2. L. E. Dickson, A new extension of Dirichlet's theorem on prime numbers, *Messenger Math.* **33** (1904), 155–161.

3. A. Dujella, There are only finitely many Diophantine quintuples, *J. Reine Angew. Math.* **566** (2004), 183–214.

4. F. Luca and I. E. Shparlinski, Approximating positive reals by ratios of kernels of consecutive integers, in *Diophantine analysis and related fields*, *Sem. Math. Sci.* **35** (Keio Univ., Yokohama, 2006). 141–148.

5. G. Tenenbaum, *Introduction to analytic and probabilistic number theory*. Cambridge Studies in Advanced Mathematics, **46** (Cambridge University Press, Cambridge, 1995).

6. D. Terr, Solution of problem H-520, *Fibonacci Quart.* **36** (1998), 94–95.