GLASNIK MATEMATIČKI
Vol. 54(74)(2019), 65 – 75

DIOPHANTINE m-TUPLES WITH THE PROPERTY $D(n)$

Riley Becker and M. Ram Murty
Queen's University, Canada

Abstract. Let n be a non-zero integer. A set of m positive integers $\{a_1, a_2, \cdots, a_m\}$ such that $a_i a_j + n$ is a perfect square for all $1 \leq i < j \leq m$ is called a Diophantine m-tuple with the property $D(n)$. In a series of papers, Dujella studied the quantity $M_n = \sup\{|\mathcal{S}| : \mathcal{S} \text{ has the property } D(n)\}$ and showed for $|n| \geq 400$ that $M_n \leq 15.476 \log |n|$ and if $|n| > 10^{100}$, then $M_n < 9.078 \log |n|$. We refine his argument to show that $C_n \leq 2 \log |n| + O\left(\frac{\log |n|}{(\log \log |n|)^2}\right)$, where the implied constant is effectively computable and $C_n = \sup\{|\mathcal{S} \cap [1, n^2]| : \mathcal{S} \text{ has the property } D(n)\}$. Together with earlier work of Dujella, this implies $M_n \leq 2.6071 \log |n| + O\left(\frac{\log |n|}{(\log \log |n|)^2}\right)$, where the implied constant is effectively computable.

1. Introduction

Let n be an non-zero integer. A set of m positive integers

$$\{a_1, a_2, \cdots, a_m\}$$

such that $a_i a_j + n$ is a perfect square for all $1 \leq i < j \leq m$ is called a Diophantine m-tuple with the property $D(n)$. Diophantus found that the quadruple

$$\{1, 33, 68, 105\}$$

has property $D(256)$. Fermat found that $\{1, 3, 8, 120\}$ has property $D(1)$ ([6]). Baker and Davenport ([1]) showed that Fermat's quadruple cannot be extended to a quintuple with property $D(1)$, and recently Dujella and others

2010 *Mathematics Subject Classification.* 11D25, 11N36.
Key words and phrases. Diophantine m-tuples, Gallagher's sieve, Vinogradov's inequality.
The first author is supported by an NSERC Undergraduate Student Research Award. The second author's research is partially supported by an NSERC Discovery grant.

showed there is no sextuple with property $D(1)$ and only finitely many, effectively computable quintuples with property $D(1)$ using sophisticated methods including Baker's theory of linear forms in logarithms ([7, 8]). Finally, in a recent paper, He, Togbé and Ziegler ([16]) have shown that there are no Diophantine quintuples. Thus, the study of Diophantine m-tuples has ancient roots, and over the centuries the methods used to study them have ranged from the very elementary to the profoundly deep.

For example, for any natural number n, we cannot have an infinite set $\{a_1, a_2, \cdots\}$ with property $D(n)$ because, by a famous theorem of Siegel ([20]), there are only finitely many integral points on the elliptic curve

$$y^2 = (a_1x + n)(a_2x + n)(a_3x + n). \tag{1.1}$$

However, known bounds for the number of integral solutions to (1.1) depend on n, a_1, a_2, and a_3.

On the other hand, if we consider the hyperelliptic curve

$$y^2 = (a_1x + n)(a_2x + n)(a_3x + n)(a_4x + n)(a_5x + n), \tag{1.2}$$

which has genus 2, a celebrated conjecture of Caporaso, Harris, and Mazur ([3]) predicts that (1.2) has a bounded number of integral points independent of n and $a_1, \cdots, a_5$. Thus, the quantity

$$M_n = \sup\{|\mathcal{S}| : \mathcal{S} \text{ has the property } D(n)\}$$

is conjectured to be bounded by an absolute constant independent of n. These observations were made by Dujella ([9]).

Some progress was made recently towards this boundedness conjecture. In [11], Dujella and Luca show that M_n is bounded in terms of the number of prime factors of n for squarefree values of n. In particular, M_p is absolutely bounded for primes p. They also show that for almost all n (in the sense of natural density), one has the estimate $M_n < \log\log|n|$.

There are other results related to this problem relevant to our discussion. For example, there is the paper by Evertse and Silverman that gives a bound for the number of integral solutions in terms of n, a_1, a_2, a_3 ([13]). Another paper of Silverman [20] connects ranks of elliptic curves to the number of integral points. In particular, if M_n is unbounded, this would suggest that there are infinitely many elliptic curves of arbitrarily large rank, resolving a celebrated open question. This remark is not a rigorous statement but is inspired by the general feeling that "an elliptic curve with many integral points must have large rank" as expressed in [20].

By very elementary congruence consideration, one can deduce that $M_n \leq 3$ if $n \equiv 2 \pmod 4$. To see this, note that

$$a_ia_j + n \equiv 0 \text{ or } 1 \pmod 4$$

since any square is congruent to either 0 or 1 (mod 4). If $n \equiv 2 \pmod 4$, we must have

$$a_i a_j \equiv 2 \text{ or } 3 \pmod 4,$$

implying that at most one a_i can be even. Then by a simple application of the pigeonhole principle, $M_n \leq 3$. This observation was made independently by Brown ([2]), Gupta and Singh ([15]) and Mohanty and Ramasamy ([17]).

Dujella ([7, 9, 10]) has written several papers dealing with estimates for M_n as a function of n. He proved that $M_n \leq 15.476 \log |n|$ if $|n| > 400$ and that if $n > 10^{100}$, then $M_n < 9.078 \log |n|$. Dujella uses a fundamental inequality due to Vinogradov (see [21, page 193]) and it seems that a sharper inequality was obtained in the Russian edition (see pages 82 and 150 of [22]). If the weaker inequality is used, then 15.476 should be replaced by 29.310 and 9.078 by 20.927. Since this subtle discrepancy may not be known to those who have the Dover English translation of [22], we will elaborate and explain the refinement. At the same time, we offer another approach to the estimate of Vinogradov which is applicable not only to quadratic characters, but also other characters as well. This will be discussed in the next section.

Dujella ([8]) decomposes his analysis into three components. He defines

$$\begin{aligned} A_n &= \sup\{|\mathcal{S} \cap [|n|^3, \infty)| : \mathcal{S} \text{ has } D(n)\} \\ B_n &= \sup\{|\mathcal{S} \cap (n^2, |n|^3)| : \mathcal{S} \text{ has } D(n)\} \\ C_n &= \sup\{|\mathcal{S} \cap [1, n^2]| : \mathcal{S} \text{ has } D(n)\} \end{aligned}$$

He proves that $A_n \leq 21$ and

$$B_n < 0.65 \log |n| + 2.24$$

for all n. He then improves these bounds in [10] to

$$B_n < 0.6071 \log |n| + 2.152$$

and

$$C_n < 11.006 \log |n|.$$

for $|n| > 400$. If $|n| > 10^{100}$, he shows that $C_n < 8.37 \log |n|$ and the final result is derived by combining all of these estimates. Since the size of A_n is globally bounded and B_n is effectively bounded by $0.65 \log |n| + 2.24$, we will henceforth focus on C_n.

In this paper, our goal is to improve the estimate for C_n:

THEOREM 1.1.

$$C_n \leq 2 \log |n| + O\left(\frac{\log |n|}{(\log \log |n|)^2}\right).$$

2. Preliminaries

In [10], the estimate for C_n was derived using Gallagher's larger sieve ([14]) together with an estimate of Vinogradov ([21]). As noted earlier Dujella ([8]) states Vinogradov's theorem from the Russian edition, omitting the 2 in Vinogradov's original statement that

$$\left|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\left(\frac{ab+n}{p}\right)\right| \leq \sqrt{2p|\mathcal{A}||\mathcal{B}|},$$

which appears in [21] and instead writing

$$\left|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\left(\frac{ab+n}{p}\right)\right| \leq \sqrt{p|\mathcal{A}||\mathcal{B}|}. \tag{2.1}$$

In a later section, we will show that (2.1) holds, but it does not follow from Vinogradov's original method ([21]) but rather from a later method explained in [22]. We will use the method of Gauss sums to derive (2.1) and it will be evident that the result holds in a more general context.

An important role is played by Gallagher's sieve estimate:

Proposition 2.1. *Let $\mathcal{S}$ be a set of integers contained in an interval of length N. Let $\mathcal{P}$ be a finite set of primes. If for each prime $p \in \mathcal{P}$, we define $u(p) = |\mathcal{S} \pmod p|$, then*

$$|\mathcal{S}| \leq \frac{\sum\limits_{p\in\mathcal{P}} \log p - \log N}{\sum\limits_{p\in\mathcal{P}} \frac{\log p}{u(p)} - \log N},$$

provided the denominator is positive.

Proof. This is [14, Theorem 1] (see also [4, Theorem 2.2.1]). □

We have written this following the formulation in [4] for ease of application and clarity.

Proposition 2.2. *Let $\theta(x) = \sum\limits_{p\leq x} \log p$, where the sum is over primes. Then*

$$|\theta(x) - x| < 3.965\frac{x}{\log^2 x}$$

for $x \geq 2$.

Proof. This is Theorem 4 of Dusart in [12]. □

Proposition 2.3.

$$\sum_{p\leq Q} \frac{\log p}{\sqrt{p}+4} = 2\sqrt{Q} + O\left(\frac{\sqrt{Q}}{\log^2 Q}\right).$$

The constant implied in the O-estimate is effectively computable.

PROOF. By partial summation, we have that

$$\sum_{p\le x} f(p)\log p = \theta(x)f(x) - \int_2^x \theta(t)f'(t)dt$$

for any function $f(t)$ which is differentiable on $[1,x]$. Applying this with $f(t) = 1/(\sqrt{t}+4)$ and using Proposition 2.2 gives the result. Indeed, we have that the sum equals

$$\frac{Q}{\sqrt{Q}+4} + O\left(\frac{\sqrt{Q}}{\log^2 Q}\right) + \int_2^Q \frac{t}{2(\sqrt{t}+4)^2}\frac{dt}{\sqrt{t}} + O\left(\int_2^Q \frac{dt}{\sqrt{t}\log^2 t}\right).$$

The first term is clearly

$$\sqrt{Q} + O(1).$$

The third term is evidently

$$\sqrt{Q} + O(\log Q).$$

Finally, the last term is estimated as follows. We break the integral into two parts:

$$\int_2^{\sqrt{Q}} + \int_{\sqrt{Q}}^Q.$$

Then, the first of these integrals is $O(Q^{1/4})$. In the second integral, we see that as $1/\log^2 t$ is a decreasing function of t, we obtain a final estimate of

$$O\left(\frac{\sqrt{Q}}{\log^2 Q}\right).$$

Using Proposition 2.2, one can derive an explicit constant implied by our O-estimate. Of course, if we invoke the prime number theorem with the best known error term, the error in our assertion can be substantially improved. □

As Dujella pointed out to us, the version of Vinogradov's theorem he used came from a later edition [22]. The improved version in the Russian edition is quite elegant and short, so we include it here for the benefit of those who do not have access to the Russian edition or do not know Russian. By Cauchy-Schwarz,

$$\left|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\left(\frac{ab+n}{p}\right)\right|^2 \le |\mathcal{A}|\sum_{a=0}^{p-1}\left|\sum_{b\in\mathcal{B}}\left(\frac{ab+n}{p}\right)\right|^2.$$

Expanding the square on the right hand side, we get

$$\left|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\left(\frac{ab+n}{p}\right)\right|^2 \le |\mathcal{A}|\sum_{b,c\in\mathcal{B}} S_{b,c},$$

where

$$S_{b,c} = \sum_{a=0}^{p-1} \left(\frac{ab+n}{p}\right)\left(\frac{ac+n}{p}\right).$$

A straightforward calculation now shows that $S_{b,c} = p$ if $b = c = 0$ and zero if $bc = 0, b \neq c$. Furthermore, if $b = c \neq 0$, then $S_{b,c} = p - 1$ and is zero otherwise. Injecting this into our sum gives

$$\left|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}} \left(\frac{ab+n}{p}\right)\right|^2 \leq |\mathcal{A}|\left((p-1)|\mathcal{B}| + \delta_{\mathcal{B}}(0)\right),$$

where

$$\delta_{\mathcal{B}}(0) = \begin{cases} 1, & \text{if } 0 \in \mathcal{B}, \\ 0, & \text{if } 0 \notin \mathcal{B}. \end{cases}$$

Of course, this implies the bound $\sqrt{p|\mathcal{A}||\mathcal{B}|}$ and is even better if $0 \notin \mathcal{B}$. A modification of this method to deal with character sums instead of quadratic sums does not lead to similar estimates (as can be verified by the reader). Indeed, the difficulty arises in the explicit computation of $S_{b,c}$ above. In the case of a non-quadratic character, one encounters Jacobi sums of the form

$$\sum_{a=0}^{p-1} \chi(a)\chi(a+t).$$

Thus, we offer below another derivation based on Gauss sums that does generalize to arbitrary characters (see Proposition 2.7).

PROPOSITION 2.4. *Let χ be a Dirichlet character (i.e. a homomorphism from $(\mathbb{Z}/p\mathbb{Z})^\times$ to $\mathbb{C}^\times$). Let*

$$\tau = \sum_{c=1}^{p} \chi(c) e^{\frac{2\pi i c}{p}}.$$

If χ is non-trivial, then $|\tau| = \sqrt{p}$. Moreover,

$$\overline{\chi}(n) = \frac{1}{\tau}\sum_{c=1}^{p-1} \chi(c) e^{\frac{2\pi n c}{p}}.$$

PROOF. This is [18, Theorem 5.3.3]. □

With this proposition we can improve upon Vinogradov's original theorem.

PROPOSITION 2.5. *Let p be an odd prime and n be an integer with $\gcd(n,p) = 1$. If $\mathcal{A} \subseteq \{1,\ldots,p-1\}$ and $\mathcal{B} \subseteq \{0,1,\ldots,p-1\}$, then*

$$\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}} \left(\frac{ab+n}{p}\right) \leq \sqrt{p|\mathcal{A}||\mathcal{B}|}.$$

PROOF. Since it will be easier to deal with the sum if the a and b are separated, we write

$$\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\left(\frac{ab+n}{p}\right)=\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\left(\frac{a}{p}\right)\left(\frac{b+na^{-1}}{p}\right).$$

Replacing $\left(\frac{b+na^{-1}}{p}\right)$ with its Gauss sum, we have

$$\begin{aligned}\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\left(\frac{ab+n}{p}\right)&=\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\left(\frac{a}{p}\right)\frac{1}{\tau}\sum_{c=0}^{p-1}\left(\frac{c}{p}\right)e^{2\pi i(b+na^{-1})c/p}\\&=\frac{1}{\tau}\sum_{c=0}^{p-1}\left(\frac{c}{p}\right)\sum_{a\in\mathcal{A}}\left(\frac{a}{p}\right)e^{2\pi ina^{-1}c/p}\sum_{b\in\mathcal{B}}e^{2\pi ibc/p}.\end{aligned}$$

Applying the Cauchy-Schwarz inequality to the right hand side, we deduce

$$\begin{aligned}&\left|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\left(\frac{ab+n}{p}\right)\right|\\&\quad\le\frac{1}{\sqrt{p}}\sum_{c=0}^{p-1}\left(\left|\sum_{a\in\mathcal{A}}\left(\frac{a}{p}\right)e^{2\pi ina^{-1}c/p}\right|^2\right)^{\frac{1}{2}}\left(\sum_{c=0}^{p-1}\left|\sum_{b\in\mathcal{B}}e^{2\pi ibc/p}\right|^2\right)^{\frac{1}{2}}\end{aligned}$$

and the right hand side is

$$\begin{aligned}&=\frac{1}{\sqrt{p}}\left(\sum_{a,a'\in\mathcal{A}}\left(\frac{aa'}{p}\right)\sum_{c=0}^{p-1}e^{2\pi in(a^{-1}-a'^{-1})c/p}\right)^{\frac{1}{2}}\left(\sum_{b,b'\in\mathcal{B}}\sum_{c=0}^{p-1}e^{2\pi i(b-b')c/p}\right)^{\frac{1}{2}}\\&=\frac{1}{\sqrt{p}}(p|\mathcal{A}|)^{1/2}(p|\mathcal{B}|)^{1/2}\\&=\sqrt{p|\mathcal{A}||\mathcal{B}|}.\end{aligned}$$

□

Now we correct this argument to include the case when $0\in\mathcal{A}$.

PROPOSITION 2.6. *Let p be an odd prime and n be an integer with* $\gcd(n,p)=1$. *If $\mathcal{A},\mathcal{B}\subseteq\{0,\dots,p-1\}$, then*

$$\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\left(\frac{ab+n}{p}\right)\le\sqrt{p|\mathcal{A}||\mathcal{B}|}+|\mathcal{B}|.$$

PROOF. Using the result of the previous proposition, we have

$$\begin{aligned}\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\left(\frac{ab+n}{p}\right)&=\sum_{a\in\mathcal{A}\setminus\{0\}}\sum_{b\in\mathcal{B}}\left(\frac{ab+n}{p}\right)+\delta_{\mathcal{A}}(0)|\mathcal{B}|\left(\frac{n}{p}\right)\\&\le\sqrt{p|\mathcal{A}||\mathcal{B}|}+|\mathcal{B}|,\end{aligned}$$

where

$$\delta_{\mathcal{A}}(a) = \begin{cases} 1, & \text{if } a \in \mathcal{A}, \\ 0, & \text{if } a \notin \mathcal{A}. \end{cases}$$

□

As hinted earlier, Proposition 2.5 is true in a wider context and we record it here:

PROPOSITION 2.7. *Let p be an odd prime and n be an integer with $\gcd(n,p)=1$. If $\mathcal{A} \subseteq \{1,\dots,p-1\}$ and $\mathcal{B} \subseteq \{0,1,\dots,p-1\}$, then*

$$\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}} \chi(ab+n) \le \sqrt{p|\mathcal{A}||\mathcal{B}|},$$

for any non-trivial character $\chi \pmod p$.

3. Proof of the Main Theorem

Let $\mathcal{S} = \{a_1, \cdots, a_m\}$, with all $a_i \le n^2 = N$. As noted earlier, this estimate for C_n combined with the estimates for A_n and B_n of [10] gives the final estimate. This is consonant with [10, Remark 4.1].

In Dujella [10], it is shown for each prime $p \le Q$ with $(p,n)=1$ that

$$|S_p| \le \min\{\sqrt{p}+3, p\},$$

where $S_p = \mathcal{S} \pmod p$. This is done using the Legendre symbol and Vinogradov's theorem as stated in equation (2.1) and showing that

$$|S_p|(|S_p|-3) \le |S_p|\sqrt{p}.$$

Using the version of the Vinogradov's theorem given in Proposition 2.6 gives instead that $|S_p|(|S_p|-3) \le |S_p|(\sqrt{p}+1)$, or that

$$|S_p| \le \sqrt{p}+4.$$

Thus, we use $u(p) = \min\{\sqrt{p}+4, p\}$ in Gallagher's sieve, noting that for $p \ge 7$, $|S_p| \le \sqrt{p}+4$. In the denominator, we have from Proposition 2.3

$$\sum_{\substack{p\le Q\\(p,n)=1}} \frac{\log p}{\sqrt{p}+4} = 2\sqrt{Q} + O\left(\frac{\sqrt{Q}}{\log^2 Q}\right) - \sum_{p|n} \frac{\log p}{\sqrt{p}+4}$$

and the final term is bounded as follows. Let p_i denote the i-th prime. Then, letting $\omega(n)$ denote the number of distinct prime divisors of n, we have again using Proposition 2.3, and noting that $\frac{\log x}{\sqrt{x}+4}$ is eventually a decreasing function,

$$\sum_{p|n} \frac{\log p}{\sqrt{p}+4} \le \sum_{i\le\omega(n)} \frac{\log p_i}{\sqrt{p_i}+4} + O(1) = 2p_{\omega(n)}^{1/2} + O\left(\frac{\sqrt{p_{\omega(n)}}}{\log^2 p_{\omega(n)}}\right) \ll (\log|n|)^{\frac{1}{2}},$$

the final estimate coming from the bound that $p_i \ll i \log i$ and Ramanujan's bound

$$\omega(n) \ll \frac{\log n}{\log \log n}.$$

Therefore

$$\sum_{\substack{p \leq Q \\ (p,n)=1}} \frac{\log p}{\sqrt{p}+4} \geq 2\sqrt{Q} + O((\log |n|)^{\frac{1}{2}}) + O\left(\frac{\sqrt{Q}}{\log^2 Q}\right).$$

We insert this into Gallagher's sieve to get an estimate for $|\mathcal{S}|$ of

$$\frac{\theta(Q) - \log N}{2\sqrt{Q} + O((\log |n|)^{\frac{1}{2}}) + O\left(\frac{\sqrt{Q}}{\log^2 Q}\right) - \log N}.$$

We choose $Q = \frac{(1+\delta)^2}{4}(\log N)^2$ so that the denominator is

$$\delta \log N + O\left(\frac{\log N}{(\log \log N)^2}\right) + O((\log |n|)^{\frac{1}{2}}) = 2\delta \log n + O((\log |n|)^{\frac{1}{2}}),$$

since $N = n^2$. Now

$$\theta(Q) = Q + O\left(\frac{Q}{\log^2 Q}\right),$$

so that the set $\mathcal{S}$ has size at most

$$2 \log |n| + O\left(\frac{\log |n|}{(\log \log |n|)^2}\right),$$

where we have chosen $\delta = 1$ to minimize the coefficient of $\log |n|$. This completes the proof.

4. Concluding remarks

There are several ways in which one can attempt to improve our estimate in the main theorem. One way is to improve the estimate of Proposition 2.5. If for example, one could show that $|S_p| = o(\sqrt{p})$, then our proof would lead to a final estimate of $o(\log |n|)$, as is readily verified by the reader.

On the other hand, the sum in Proposition 2.5 is trivially less than or equal to $|A||B|$. If one could improve this to $\delta|A||B|$, for any $\delta < 1$, then one can deduce boundedness of M_n for all values of n. Indeed, following Dujella [10],

$$|S_p|^2 - 3|S_p| \leq \sum_{a \in S_p} \sum_{b \in S_p} \left(\frac{ab+n}{p}\right) < \delta |S_p|^2,$$

implies $|S_p| \leq 3/(1-\delta)$ so that S_p is bounded. Injecting this into our argument above leads to the boundedness of C_n and B_n and consequently M_n. The point is that to include B_n in the analysis, we need to take $N = n^3$ and Q is chosen to be a sufficiently large multiple of $\log N$.

It is possible to determine the implied constant in the O-estimate of our main theorem using Proposition 2.2 and partial summation. To keep our derivation reasonably elegant, we have not done so here. Of course, using the prime number theorem with error term, one could replace this error by

$$O((\log |n|)e^{-c\sqrt{\log\log |n|}})$$

for some $c > 0$. Though there are sharp effective error terms, computing precise numerical constants is quite cumbersome. For the ambitious reader, we suggest reasonably painless path to derive explicit constants.

We need a lower bound for

$$\sum_{7\leq p\leq Q,(p,n)=1} \frac{\log p}{\sqrt{p}+4}.$$

This is easily seen to be

$$\geq \sum_{7\leq p\leq Q,(p,n)=1} \frac{\log p}{\sqrt{p}} - 4\sum_{7\leq p\leq Q} \frac{\log p}{p}.$$

These sums are more amenable for the insertion of Dusart's explicit estimates via partial summation. The only snag is that we also need to estimate the sum

$$\sum_{p|n} \frac{\log p}{\sqrt{p}}$$

which of course can be dealt with the more explicit estimates for the i-th prime and $\omega(n)$ in the form

$$p_i < i\log i + i\log\log i$$

for $i \geq 6$. Also, one can apply an estimate due to Robin ([19]): for $n \geq 3$,

$$\omega(n) \leq \frac{\log n}{\log\log n} + 1.45743\frac{\log n}{(\log\log n)^2}.$$

We leave the details to the assiduous reader.

Acknowledgements.

We thank Andrej Dujella for his comments on an earlier version of our paper as well as bringing [22] to our attention. We also thank Ahmet Güloğlu and the referees for their helpful and meticulous corrections and suggestions.

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. (2) **20** (1969), 129–137.

[2] E. Brown, *Sets in which* $xy + k$ *is always a square*, Math. Comp. **45** (1985), 613–620.

[3] L. Caporaso, J. Harris and B. Mazur, *Uniformity of Rational Points*, J. Amer. Math. Soc. **10** (1997), 1–35.

[4] A. C. Cojocaru and M. R. Murty, An introduction to sieve methods and their applications, Cambridge University Press, 2006.
[5] H. Davenport, Multiplicative number theory, Springer-Verlag, New York, 1980.
[6] L. E. Dickson, History of the theory of numbers, Washington Carnegie Institution of Washington, 1923, 513–520.
[7] A. Dujella, *An absolute bound for the size of Diophantine m-tuples*, J. Number Theory **89** (2001), 126–150.
[8] Andrej Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. **566** (2004), 183-214.
[9] A. Dujella, *On the size of Diophantine m-tuples*, Math. Proc. Cambridge Philos. Soc. **132** (2002), 23–33.
[10] A. Dujella, *Bounds for the size of sets with the property $D(n)$*, Glas. Mat. Ser. III **39(59)** (2004), 199–205.
[11] A. Dujella and F. Luca, *Diophantine m-tuples for primes*, Int. Math. Res. Not. **47** (2005), 2913–2940.
[12] P. Dusart, *Explicit estimates of some functions over primes*, Ramanujan J. **45** (2018), 227–251.
[13] J.-H. Evertse and J. H. Silverman, *Uniform bounds for the number of solutions to $Y^n = f(X)$*, Math. Proc. Cambridge Philos. Soc. **100** (1986), 237–248.
[14] P. X. Gallagher, *A larger sieve*, Acta Arith. **18** (1971), 77–81.
[15] H. Gupta and K. Singh, *On k-triad sequences*, Internat. J. Math. Math. Sci. **8** (1985), 799–804.
[16] B. He, A. Togbé and V. Ziegler, *There is no Diophantine quintuple*, Trans. Amer. Math. Soc. **371** (2019), 6665–6709.
[17] S. P. Mohanty and A. M. S. Ramasamy, *On $P_{r,k}$ sequences*, Fibonacci Quart. **23** (1985), 36–44.
[18] M. R. Murty, Problems in analytic number theory, Springer, New York, 2008.
[19] G. Robin, *Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n* , Acta Arit. **42** (1983), 367–389.
[20] J. H. Silverman, *A quantitative version of Siegel's theorem: integral points on elliptic curves and Catalan curves,* J. Reine Angew. Math. **378** (1987), 60–100.
[21] I. M. Vinogradov, Elements of number theory, Dover Publications, Inc., New York, 1954.
[22] I. M. Vinogradov, Elements of number theory (Russian), St. Petersburg, 2004.

R. Becker
Department of Mathematics
Queen's University
Kingston, Ontario, K7L 3N6
Canada
E-mail: rileydbecker@gmail.com

M. R. Murty
Department of Mathematics
Queen's University
Kingston, Ontario, K7L 3N6
Canada
E-mail: murty@queensu.ca

Received: 20.8.2018.
Revised: 24.1.2019.