数理解析研究所講究録
第2014巻 2017年 124-131

A wishlist for Diophantine quintuples

Tim Trudgian*

Dedicated to Hideaki Ishikawa and Yuichi Kamiya for organising an excellent conference in Kyoto.

Abstract

We are concerned with Diophantine quintuples, that is, sets $\{a, b, c, d, e\}$ of distinct positive integers the product of any two of which is one less than a perfect square. We present some recent progress in the area and give a series of 9 'wishes' for future research on the topic.

1 Introduction

Consider the set $\{1, 3\}$: the product of its two elements is one less than a perfect square: call this a *Diophantine double*. Now add the number 8: the set $\{1, 3, 8\}$ (still) has the property that the product of any two of its elements is one less than a perfect square: call this a *Diophantine triple*. In general a Diophantine m-tuple, or simply an m-tuple is a set of m distinct integers the product of any two of which is one less than a perfect square. While $\{1, 3, 8, 120\}$ illustrates the existence of quadruples (and there are infinitely many), it is conjectured that *there are no quintuples* $\{a, b, c, d, e\}$, with $a < b < c < d < e$.

A brief sketch of the Diophantine quintuple problem, as well as a table giving various bounds on the number of quintuples is given in [12]. Attempts to show there are no quintuples $\{a, b, c, d, e\}$ use the following recipe.

1. Use an effective version of Baker's theorem (or similar) on linear forms of logarithms. This produces a bound on d. This bounds the *size* of the quintuples.

2. Use some techniques from elementary and analytic number theory. This converts the *size* of the quintuples into an estimate on their *number*.

*Supported by Australian Research Council DECRA Grant DE120100173.

The best bounds to date on d and on N_q, the total number of quintuples, appear in [3] and are

$$d < 7.3 \cdot 10^{67}, \quad N_q < 5.5 \cdot 10^{26}. \tag{1}$$

Step 1 allows one, at least in principle, to enumerate all quadruples $\{a, b, c, d\}$ that *may* be extendable to quintuples. The goal is then to show, using solutions to Pell equations, congruence conditions, or some computation, that no quadruple in this list can be so extended.

A lot of work in recent papers ([5], [2], [12], [3]) has focussed on Step 2. While one can make more substantial savings by addressing Step 1, gains from using Step 2 are far from exhausted.

Martin and Sitar [9] showed that the number of quadruples $\{a, b, c, d\}$ with $d \leq x$ is asymptotically

$$Cx^{1/3} \log x, \quad C = \frac{2^{4/3}}{3\Gamma(2/3)^2} = 0.338285\ldots. \tag{2}$$

Fujita [6] showed that there are at most four ways of extending a given quadruple into a quintuple. In the worst-case scenario when each quadruple could be extended to four quintuples, and assuming that the lower order terms in (2) are negligible, the bounds on d in (1) give the estimate $N_q < 8.9 \cdot 10^{24}$. This is about a factor of 60 better than the bound in (1).

2 The Wishlist

The goal of this section is not to furnish the absolute best bounds obtainable given the suggested improvements. It is often the case that the best bounds are obtained through an optimisation process, coupled with some computation. Rather than pursue this, we have merely outlined the estimated size of the improvements.

2.1 Linear forms of logarithms

Matveev [10] has given a completely explicit version of Baker's theorem of linear forms of logarithms. This is for n logarithms and for number fields of degree d. While it looks difficult to improve his theorem by much for arbitrary n and d, for the quintuple problem we need only consider $n = 3$ and $d = 4$. For these values, one finds a very large 'constant' in Matveev's theorem, namely $1.73 \cdot 10^{11}$, which can be seen in [12, (16)].

Wish 1. *Reduce Matveev's constant from* $1.73 \cdot 10^{11}$ *by specialising the proof when* $n = 3$ *and* $d = 4$.

Reducing Matveev's constant C has a significant impact on the bounds for d and N_q: this is illustrated in Table 1.

Table 1: Matveev's constant C and upper bounds for d and N_q

C	d	N
10^{11}	$1.3 \cdot 10^{67}$	$3 \cdot 10^{27}$
10^{10}	$5.5 \cdot 10^{62}$	$2 \cdot 10^{26}$
10^{9}	$2.3 \cdot 10^{58}$	$2 \cdot 10^{24}$
10^{8}	$8.8 \cdot 10^{53}$	$7 \cdot 10^{22}$
10^{7}	$3.1 \cdot 10^{49}$	$2 \cdot 10^{21}$
10^{6}	$9.7 \cdot 10^{44}$	$7 \cdot 10^{19}$

Baker's theorem has also been made explicit by Alexentsev [1]. For the quintuples problem this yields a slightly smaller constant than Matveev's result, and indeed was used in [12] and [3] to make a small improvement over that in [2]. Alexsentsev's results differ slightly from Matveev's in the form of quantities E and B, which are too complicated to be mentioned here, but which are related to heights of algebraic numbers. We simply conclude that variants exist, and one may be able to inject ideas of Waldschmidt [13] to improve on the estimates of d and N_q.

Wish 2. *Use different versions Matveev's/Alexenstev's results to yield superior results.*

We remark that this is distinct from reducing the size of the constant as in Wish 1.

Finally, there is the so-called 'kit for logarithms' as given by Mignotte [11]. This, in principle, allows one to use results on sums of two logarithms to improve estimates on sums of three logarithms. Since the numerical constants in the two-log case are far superior this is an attractive option.

Wish 3. *Use results for two logarithms in the quintuples problem.*

2.2 Eliminating small values of a

Given a bound on d one obtains bounds on a and b, and then deduces bounds on the number of doubles $\{a, b\}$. This feeds into the ultimate bound on N_q. The bounds on b, and hence the overall bound on N_q, is the worst for $a = 1$: in general, small values of a contribute the most to N_q. It is therefore desirable to eliminate, or at least mitigate the impact of, these small values of a.

Wish 4. *Show that there can be no quintuples with $a = 1$.*

This appears to be "wishful" thinking at the present. In the absence of such a proof one seeks at minimising the damage wrought by these small values of a. To that end, one can consider $a = 1, 2, 3$, say, separately from $a \geq 4$. For this section only, consider $a = 1$.

Jones [8] proved that $c > 4b$; this was improved slightly by Cipu [2] to $c > 5b + 1$. Actually, Jones proved that $c > 4bc'$ where $c' + 1 = y'^2$, where

$$y' = \sqrt{b+1}\sqrt{c+1} - \sqrt{bc+1}, \tag{3}$$

after which Jones concluded that $c' > 1$. If $c \geq \lambda b$ then, since (3) is increasing in c, we have that

$$y' \gtrsim \frac{\sqrt{\lambda}}{2}\left(1 + \frac{1}{\lambda}\right), \tag{4}$$

where we have neglected some small, lower-order terms. Since we have $c > 5b$ we can take $\lambda = 5$ in (4). This shows that $y' \geq 1.34$ and so, since y' must be an integer, we have $y' \geq 2$.

This shows that $c' \geq 3$, whence $c \geq 12b$. We therefore deduce that $c \geq 12b$. This lower bound for c will reduce the overall bound on d slightly. There is a 'force multiplier effect' at work here: the reduction on d reduces N_q, but also, the lower bound on c has a 'direct' effect at reducing N_q.

Wish 5. *Continue this scheme of bounding c when a is small, and lower the overall bound on N_q.*

2.3 Bounds on $2^{\omega(b)}$

In [5] and in all subsequent papers on the subject, one considers the maximal number of distinct prime factors of b. In [3] we have $b < 1.91 \cdot 10^{33}$, which means that b could have as many as 23 distinct prime factors. This induces a factor of 2^{23} in the overall bound on the number of quintuples.

Removing k prime factors from b improves the final result by a factor of 2^k. In [3, (20)] the following problem was presented: enumerate all b such that

$$\prod_{i=1}^{23} p_i \approx 2.67 \cdot 10^{32} \leq b < 1.91 \cdot 10^{33}, \quad \omega(b) = 23, \tag{5}$$

where the product is over the first 23 primes. It was shown in [3] that none of the values of b in (5) could be extended to a quintuple; whence we deduce that b has at most 22 prime factors, and so the final bound on the number of quintuples is halved.

One should now like to enumerate

$$\prod_{i=1}^{22} p_i \approx 3.22 \cdot 10^{30} \leq b < 1.91 \cdot 10^{33}, \quad \omega(b) = 22, \tag{6}$$

and try to eliminate these, as before. Given the much larger spread of values of b in (6), this is a harder task than earlier, but nevertheless this leads us to

Wish 6. *Eliminate another distinct prime factor of b, and hence reduce the bound on N_q by a factor of 2.*

2.4 More cases, more congruences

By [3, Lem. 2.4] any potential quintuple arises from one of four possible triples: these triples were labelled cases A, B, C, and D. The largest contribution to N_q came from quintuples from case A; the smallest from case D.

At the RIMS conference in Kyoto I offered 1000 yen for the proof that no quintuples could come from case D triples. It is a delight to record here that Yasutsugu Fujita and Takafumi Miyazaki [7] should be able to claim that prize at next year's meeting. They actually eliminated cases B and D from consideration. Therefore we know that *any* quintuple $\{a, b, c, d, e\}$ must have

$$b > 4a, \quad c > 4ab + b + a.$$

In [3] this was partitioned into two categories: case A being those with $c < b^{3/2}$ and case C being the rest. One could create new case A′ with $c < b^{\eta}$ for some η and case C′ being the rest. It is known [2, Prop. 3.1] that $\eta \leq 3$.

Wish 7. *Show that all quintuples must satisfy $b > 4a$ and $c < b^{\eta}$ for some $\eta \in (3/2, 3)$.*

By partitioning quintuples in such a way, their overall number is likely to decrease.

2.5 Explicit arithmetical sums

In bounding the number of quintuples one makes use of sums of the form $\sum_{n \leq x} 2^{\omega(n)}$. For most of these sums, the asymptotic size is well-known, but explicit upper bounds are difficult to find. Recently, Dudek [4] proved that

$$\sum_{2 \leq n \leq N} d(n^2 - 1) \sim \frac{6}{\pi^2} N \log^2 N. \tag{7}$$

This can be put to work in estimating the number of doubles $\{a, b\}$ with $a < b \leq N$. In [3], (7) was made explicit, viz. for $N \geq 2$ we have

$$\sum_{2 \leq n \leq N} d(n^2 - 1) \leq \frac{6}{\pi^2} N \log^2 N + 2.369 N \log N + \dots, \tag{8}$$

where the lower order terms are explicitly given. The explicit inequality in (8) matches the one in (7) to the first term. Although the lower-order terms in (7) are not yet known, almost certainly the lower-order terms in (8) are excessive. Therefore, there is something to be gained by pursuing

Wish 8. *Calculate the lower-order terms in* $\sum d(n^2 - 1)$. *Probably the first is* $c_1 N \log N \dots$, *for some positive constant* c_1. *Now try to obtain an explicit upper bound on* $\sum d(n^2 - 1)$ *in which the second term is* $c_1 N \log N$.

Currently, in examining quintuples from Case C, one uses the bound

$$\sum_{n \leq N} 4^{\omega(n)} \leq \sum_{n \leq N} d_4(n) \leq \frac{N}{6} (\log N + 2)^3. \tag{9}$$

In [12] I showed that

$$\sum_{n \leq N} 4^{\omega(n)} \sim \frac{H_0}{6} N \log^3 N, \quad H_0 = 0.1148 \dots, \tag{10}$$

where H_0 is an exact constant arising from a product over primes. Koichi Kawada, succeeded in winning the 100 yen prize I set for the problem of improving on the bound in (9). The key to Kawada's bound is in writing

$$k^{\omega(n)} = \sum_{d|n} \mu(d)^2 (k-1)^{\omega(d)},$$

whence, after a moderate amount of work, one can show that

$$\sum_{n \leq N} 4^{\omega(n)} \leq N \left(\frac{45}{2\pi^6} \log^3 N + A_1 \log^2 N + A_2 \log N + A_3 \right), \tag{11}$$

where $N \geq 2$ and where the A_i are explicit constants satisfying

$$A_1 < 0.6252, \quad A_2 < 3.317, \quad A_3 < 1.485.$$

This improves on the bound in (9) for all $N \geq 8$.

Wish 9. *Find an explicit version of (10) or, failing that, derive a sharper version of (11).*

It is likely that, were one to partition Cases A and C judiciously, one could use Wish 9 to reduce N_q.

Acknowledgements

It is my pleasure to acknowledge the sustained collaboration and suggestions of Mihai Cipu on all matters quintuple. I should like to thank

- Yasutsugu Fujita and Takafumi Miyazaki for interesting discussions on quintuples at RIMS, and also for an advanced copy of their paper.
- Paul Voutier for discussions, suggestions, and for bringing Michel Waldschmidt's paper [13] to my attention.
- Koichi Kawada who provided the estimate in (11).

References

[1] Y. M. Aleksentsev, The Hilbert polynomial and linear forms in the logarithms of algebraic numbers, *Izv. Math.* **72** (2008), 1063–1110.

[2] M. Cipu, Further remarks on Diophantine quintuples, *Acta Arith.* **168** (2015), 201–219.

[3] M. Cipu and T. Trudgian, Searching for Diophantine quintuples. *Acta Arith.*, to appear.

[4] A. Dudek. On the number of divisors of $n^2 - 1$. *Bull. Aust. Math. Soc.* **93** (2016), 194–198.

[5] C. Elsholtz, A. Filipin, Y. Fujita, On Diophantine quintuples and $D(-1)$-quadruples, *Monats. Math.* **175** (2014), 227–239.

[6] Y. Fujita, The number of Diophantine quintuples, *Glas. Mat. Ser. III* **45** (2010), 15–29.

[7] Y. Fujita and T. Miyazaki, The regularity of Diophantine quadruples. Preprint.

[8] B. W. Jones, A second variation on a problem of Diophantus and Davenport, *Fibonacci Quart.* **16** (1978), 155–165.

[9] G. Martin and S. Sitar, Erdős–Turán with a moving target, equidistribution of roots of reducible quadratics, and Diophantine quadruples. *Mathematika*, **57**(1) (2011), 1–29.

[10] E. M. Matveev, An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II, *Izv. Math.* **64**(6) (2000), 1217–1269.

[11] M. Mignotte. A kit on linear forms in three logarithms, 45 pp, available at `http://www-irma.u-strasbg.fr/?bugeaud/travaux/kit.ps`.

[12] T. S. Trudgian, Bounds on the number of Diophantine quintuples, *J. Number Theory* **157** (2015), 233–249.

[13] M. Waldschmidt, Minorations de combinaisons linéaires de logarithmes de nombres algébriques. *Canad. J. Math.*, **45**(1) (1993), 176–224.

Tim Trudgian
Mathematical Sciences Institute
The Australian National University, ACT 0200, Australia
E-mail address: timothy.trudgian@anu.edu.au