THE UNIQUE EXTENSIONS OF TWO PARAMETRIC FAMILIES OF DIOPHANTINE TRIPLES

MIHAI CIPU, YASUTSUGU FUJITA, AND MAURICE MIGNOTTE

Abstract. This note gives a summary of the paper [5]. For a nonzero integer n, a set of m positive integers is called *a $D(n)$-m-tuple* if the product of any two distinct elements increased by n is a perfect square. Let A, K be positive integers and $\varepsilon \in \{-2,-1,1,2\}$. The main theorem of this note asserts that each of the $D(\varepsilon^2)$-triples $\{K, A^2K+2\varepsilon A, (A+1)^2K+2\varepsilon(A+1)\}$ has unique extension to a $D(\varepsilon^2)$-quadruple.

1. Main Theorem

Let n be a nonzero integer. A set $\{a_1, \ldots, a_m\}$ of m distinct positive integers is called *a $D(n)$-m-tuple* if a_ia_j+n is a perfect square for all i, j with $1 \le i < j \le m$. In the case where $n=1$, it is also called *a Diophantine m-tuple*. The first example of a Diophantine quadruple, viz., $\{1,3,8,120\}$, was found by Fermat. Euler generalized it to get the Diophantine quadruple $\{a, b, a+b+2r, 4r(r+a)(r+b)\}$, where $\{a,b\}$ is an arbitrary Diophantine pair with $r=\sqrt{ab+1}$. Thus, any Diophantine pair can be extended to a Diophantine quadruple. Note that the second largest element $a+b+2r$ in the quadruple is known to be the smallest among all the possible elements $c > \max\{a,b\}$ extending a fixed Diophantine pair $\{a,b\}$ into a Diophantine triple (cf. [16, Lemma 4]).

While there exist infinitely many Diophantine quadruples, a folklore conjecture states that there exists no Diophantine quintuple. Very recently, He, Togbé and Ziegler announced that they settled this conjecture (cf. [15]).

There is a stronger conjecture than the folklore one, which is still open. Arkin, Hoggatt and Strauss (cf. [1]), and independently Gibbs (cf. [12]), found that for any Diophantine triple $\{a,b,c\}$ with $r=\sqrt{ab+1}$, $s=\sqrt{ac+1}$ and $t=\sqrt{bc+1}$, the set $\{a,b,c,d_+\}$ is always a Diophantine quadruple, where $d_+ = a+b+c+2(abc+rst)$. Such a quadruple is called *regular*, and it is conjectured that any Diophantine quadruple is regular (cf. [1], [12]). Note that the largest element d_+ in the quadruple is known to be the smallest among all the possible elements $d > \max\{a,b,c\}$ extending a fixed Diophantine triple $\{a,b,c\}$ into a Diophantine quadruple (cf. [7, Proposition 1]).

In 1969, Baker and Davenport showed that if $\{1,3,8,d\}$ is a Diophantine quadruple, then $d=120$, which is d_+ in the above notation. Thus, their result supports the validity of the stronger conjecture. There are various kinds of generalizations of this result. For example, it is shown by He and Togbé that if $\{K, A^2K+2A, (A+1)^2K+2(A+1), d\}$ is a Diophantine quadruple with positive

2010 *Mathematics Subject Classification.* 11D09, 11B37, 11J68, 11J86.

Key words and phrases. Diophantine m-tuples, Pellian equations, hypergeometric method, linear forms in logarithms.

The second author is partially supported by JSPS KAKENHI Grant Number 16K05079.

integers K and A satisfying either $A \le 10$ or $A \ge 52330$, then $d = d_+$ (cf. [13], [14]).

The case where $n = 4$ can be discussed analogously to the case where $n = 1$. There are conjectures saying that there exists no $D(4)$-quintuple and that if $\{a, b, c, d\}$ is a $D(4)$-quadruple with $r = \sqrt{ab+4}$, $s = \sqrt{ac+4}$ and $t = \sqrt{bc+4}$, then $d = d_+$, where $d_+ = a + b + c + (abc + rst)/2$. Such a quadruple is called also *regular*. Moreover, it is shown by Filipin, He and Togbé in [10] that if $\{K, A^2K + 4A, (A+1)^2 + 4(A+1), d\}$ is a $D(4)$-quadruple with positive integers K and A satisfying $A \le 22$ and $A \ge 51767$, then $d = d_+$.

Other generalizations and exhaustive references can be seen on Dujella's webpage ([8]).

Our main theorem below generalizes the above results on the extensibilities of both families of $D(1)$- and $D(4)$-triples.

Main Theorem. (cf. [5, Theoren 1]) *Let A, K be positive integers. If $\{K, A^2K + 2\varepsilon A, (A+1)^2K + 2\varepsilon(A+1), d\}$ is a $D(\varepsilon^2)$-quadruple with $\varepsilon \in \{-2, -1, 1, 2\}$, then it is regular, in other words, we have*

$$d = d_+ = \varepsilon^{-2}(2A^2 + 2A)^2K^3 + \varepsilon^{-1}(16A^3 + 24A^2 + 8A)K^2 + (20A^2 + 20A + 4)K + \varepsilon(8A + 4). \tag{1.1}$$

Note that it suffices to show the theorem for $\varepsilon \in \{\pm 2\}$, since for any $D(1)$-triple $\{k, A^2k \pm 2A, (A+1)^2k \pm 2(A+1)\}$, the set $\{K, A^2K \pm 4A, (A+1)^2K \pm 4(A+1)\}$ is a $D(4)$-triple with $K = 2k$, which is obtained from our triple $\{K, A^2K + 2\varepsilon A, (A+1)^2K + 2\varepsilon(A+1)\}$ by substituting $\varepsilon = \pm 2$.

The key to proving Main Theorem is to optimize Rickert's theorem (cf. [19]) on simultaneous rational approximations to irrationals with consideration for the peculiarities of the two parametric families.

Main Theorem has the following immediate corollary.

Corollary 1. (cf. [5, Corollary 2]) *Let $\tau \in \{1, 2\}$. Let $\{a, b, c, d\}$ be a $D(\tau^2)$-quadruple with $a < b < c$ and $c = a + b + 2r$, where $r = \sqrt{ab + \tau^2}$. If $r \equiv \pm\tau \pmod{a}$, then $d = d_+$. In particular, if a has either of the forms 4τ, p^e and $2p^e$ with p an odd prime and e a non-negative integer, then $d = d_+$.*

The proof of Corollary 1 will be given at the end of this note. The remaining part of this note will be devoted to proving Main Theorem on the assumption that $\boxed{\varepsilon = -2}$, since the case $\varepsilon = 2$ can be treated similarly.

2. Application of Laurent's theorem

Let $a = K$, $b = A^2K - 4A$ and $c = (A+1)^2K - 4(A+1)$. Then, $r = AK - 2$, $s = (A+1)K - 2$ and $t = A(A+1)K - 2(2A+1)$. Assume that $\{a, b, c, d\}$ is a $D(4)$-quadruple with $d > d_+$. Let x, y and z be positive integers satisfying $ad + 4 = x^2$, $bd + 4 = y^2$ and $cd + 4 = z^2$. Eliminating d from these equalities leads us to the following system of Pellian equations:

$$ay^2 - bx^2 = 4(a - b), \tag{2.1}$$

$$az^2 - cx^2 = 4(a - c), \tag{2.2}$$

$$bz^2 - cy^2 = 4(b - c). \tag{2.3}$$

As is well-known, any positive solution to each of Pellian equations (2.1) to (2.3) can be expressed as a linear recurrence sequence whose initial term has only finitely may possibilities. More precisely, e.g., all positive solutions to (2.2) and (2.3) are respectively described as $z = v_m$ and $z = w_n$, where

$$v_0 = z_0,\ v_1 = \frac{1}{2}(sz_0 + cx_0),\ v_{m+2} = sv_{m+1} - v_m,$$

$$w_0 = z_1,\ w_1 = \frac{1}{2}(tz_1 + cy_1),\ w_{n+2} = tw_{n+1} - w_n,$$

for some integers m, n and some solutions (z_0, x_0), (z_1, y_1) (called *fundamental solutions*) to (2.2), (2.3), respectively, with

$$|z_0| < a^{-1/4}c^{3/4}, \quad |z_1| < b^{-1/4}c^{3/4} \tag{2.4}$$

(cf. [6, Lemma 1]). Considering the congruence $v_m \equiv w_n \pmod{2c}$ together with inequalities (2.4), we see that $m \equiv n \equiv 0 \pmod 2$, $x_0 = y_1 = 2$ and $z_0 = z_1 = \pm 2$ (cf. [5, Lemma 9]). Then, a similar argument gives the fundamental solutions to (2.1), (2.3) and the attached sequences $\{u'_n\}$, $\{u''_l\}$ with $y = u'_n = u''_l$ explicitly (cf. [5, Lemma 10]). Finally, we deduce that any positive solutions to (2.1), (2.2) can be expressed as $x = V_{2l} = W_{2m}$ for some integers l, m (note that we replaced l, m by $2l$, $2m$ since $l \equiv m \equiv 0 \pmod 2$ can be proved), where

$$V_0 = 2,\ V_1 = r + a,\ V_{l+2} = rV_{l+1} - V_l,$$
$$W_0 = 2,\ W_1 = s \pm a,\ W_{m+2} = sW_{m+1} - W_m.$$

The standard technique (see, e.g., [2]) allows us to transform the equation $V_{2l} = W_{2m}$ into the estimates

$$0 < \Lambda := 2l \log\beta - 2m \log\alpha + \log\chi < \alpha^{1-4m}, \tag{2.5}$$

where

$$\alpha = \frac{s + \sqrt{ac}}{2}, \quad \beta = \frac{r + \sqrt{ab}}{2}, \quad \chi = \frac{\sqrt{bc} + \sqrt{ac}}{\sqrt{bc} \pm \sqrt{ab}}.$$

Putting $\nu := l - m$, which can be shown to be positive, we may rewrite $\varLambda$ as

$$\varLambda = \log(\beta^{2\nu}\chi) - 2m\log(\alpha/\beta). \tag{2.6}$$

Since α and β are similar in size, we obtain the following strong lower bound for m.

Lemma 2. (cf. [5, Lemma 17]) $m > (A - 1)\nu \log\beta$.

Proof. By (2.5) and (2.6), we have $m \log(\alpha/\beta) > \nu \log\beta$. Since the mean value theorem tells us that $\log(\alpha/\beta) = f'(\xi)(s - r)$ for some $\xi \in \mathbb{R}$ with $r < \xi < s$ (where $f(u) := \log((u + \sqrt{u^2 - 4})/2)$), $s - r = a$ and

$$f'(\xi) = \frac{1}{\sqrt{\xi^2 - 4}} < \frac{1}{\sqrt{r^2 - 4}} = \frac{1}{\sqrt{ab}},$$

we obtain $\log(\alpha/\beta) < \sqrt{a/b} < 1/(A - 1)$. □

Now we appeal to Laurent's theorem on linear forms in two logarithms of algebraic numbers.

Lemma 3. (cf. [17, Theorem 2]) *Let γ_1 and γ_2 be multiplicatively independent algebraic numbers with $|\gamma_1| \geq 1$ and $|\gamma_2| \geq 1$. Let b_1 and b_2 be positive integers. Consider the linear form in two logarithms:*

$$\Lambda = b_2 \log \gamma_2 - b_1 \log \gamma_1,$$

where $\log \gamma_1, \log \gamma_2$ are any determinations of the logarithms of γ_1, γ_2 respectively. Let ρ and μ be real numbers with $\rho > 1$ and $1/3 \leq \mu \leq 1$. Set

$$\sigma = \frac{1 + 2\mu - \mu^2}{2}, \quad \lambda = \sigma \log \rho.$$

Let a_1, a_2 be real numbers such that

$$\begin{aligned} &a_i \geq \max\{\, 1,\ \rho\,|\log \gamma_i| - \log|\gamma_i| + 2D\,\mathrm{h}(\gamma_i)\,\} \quad (i = 1, 2), \\ &a_1 a_2 \geq \lambda^2, \end{aligned}$$

where $D = [\mathbb{Q}(\gamma_1, \gamma_2) : \mathbb{Q}]\,/\,[\mathbb{R}(\gamma_1, \gamma_2) : \mathbb{R}]$. Let h be a real number such that

$$h \geq \max\left\{ D\left(\log\left(\frac{b_1}{a_2} + \frac{b_2}{a_1}\right) + \log \lambda + 1.75\right) + 0.06,\ \lambda,\ \frac{D \log 2}{2} \right\}.$$

Then we have

$$\log|\Lambda| \geq C\left(h + \frac{\lambda}{\sigma}\right)^2 a_1 a_2 + \sqrt{\omega\theta}\left(h + \frac{\lambda}{\sigma}\right) + \log\left(C'\left(h + \frac{\lambda}{\sigma}\right)^2 a_1 a_2\right),$$

where

$$\begin{aligned} \sigma &= \frac{1 + 2\mu - \mu^2}{2}, \quad \lambda = \sigma \log \rho, \\ \omega &= 2\left(1 + \sqrt{1 + \frac{1}{4H^2}}\right), \quad \theta = \sqrt{1 + \frac{1}{4H^2}} + \frac{1}{2H}, \\ H &= \frac{h}{\lambda} + \frac{1}{\sigma}, \\ C &= \frac{\mu}{\lambda^3 \sigma}\left(\frac{\omega}{6} + \frac{1}{2}\sqrt{\frac{\omega^2}{9} + \frac{8\lambda\omega^{5/4}\theta^{1/4}}{3\sqrt{a_1 a_2} H^{1/2}} + \frac{4}{3}\left(\frac{1}{a_1} + \frac{1}{a_2}\right)\frac{\lambda\omega}{H}}\right)^2, \\ C' &= \sqrt{\frac{C\sigma\omega\theta}{\lambda^3 \mu}}. \end{aligned}$$

Proposition 4. (cf. [5, Proposition 28]) *Let $a = K$, $b = A^2K - 4A$, $c = (A + 1)^2K - 4(A + 1)$ with positive integers A, K. Suppose that $\{a, b, c, d\}$ is a $D(4)$-quadruple with $d > 2$ not given by (1.1). Then, we have $A \leq 2800$.*

Proof. Applying Lemma 3 to Λ with $b_1 = 2m$, $b_2 = 1$, $\gamma_1 = \alpha/\beta$ and $\gamma_2 = \beta^{2\nu}\chi$, we obtain

$$\frac{m}{(40\nu + 0.058)\log \beta} < 69.88, \tag{2.7}$$

which together with Lemma 2 yields $A \leq 2800$. □

3. Application of Rickert's theorem

Consider equations (2.2) and (2.3). Put $N = (A^2 + A)K/2 - 2A$, $\theta_1 = \sqrt{1 + 2A/N}$ and $\theta_2 = \sqrt{1 - 2/N}$.

Lemma 5. (cf. [5, Lemma 26])

$$\max\left\{\left|\theta_1 - \frac{(A+1)x}{z}\right|, \left|\theta_2 - \frac{(A+1)y}{Az}\right|\right\} < 2(A+1)\left(A+1+\frac{2}{K}\right)z^{-2}.$$

Proof. Use the equalities

$$\theta_1 = (A+1)\sqrt{\frac{a}{c}}, \quad \theta_2 = \frac{A+1}{A}\sqrt{\frac{b}{c}},$$

and the fact that $\sqrt{a/c}$, $\sqrt{b/c}$ are similar in size to x/z, y/z, respectively, in view of equations (2.2), (2.3). □

The following is a version of Rickert's theorem (cf. [19]).

Theorem 6. (cf. [5, Theorem 5]) *Let A, K be integers satisfying $A \geq 2$ and $K \geq 240.24(A+1)$. Put $N = (A^2+A)K/2 - 2A$. Then the numbers $\theta_1 = \sqrt{1 + 2A/N}$ and $\theta_2 = \sqrt{1 - 2/N}$ satisfy*

$$\max\left\{\left|\theta_1 - \frac{p_1}{q}\right|, \left|\theta_2 - \frac{p_2}{q}\right|\right\} > \left(2.838 \cdot 10^{28}(A+1)N\right)^{-1} q^{-\lambda}$$

for all integers p_1, p_2, q with $q > 0$, where

$$\lambda = 1 + \frac{\log(20(A+1)N)}{\log\left(\frac{0.669N^2}{4A(A+1)}\right)} < 2.$$

Note that in [10], where the family with $\varepsilon = 2$ is considered, in order to apply a version of Rickert's theorem ([10, Theorem 3]) with $\lambda < 2$ it is necessary to assume $K > 0.64A(A+1)^3$, which is in general much stronger than the assumption $K \geq 240.24(A+1)$ in Theorem 6. Such an improvement comes from the following facts:

- $N \equiv 0 \pmod{A}$;
- $N + 2A \equiv N - 2 \equiv 0 \pmod{(A+1)}$.

These divisibility properties largely reduce the denominators of coefficients of a Padé approximation to $\theta_1(x)$ and $\theta_2(x)$ valued at $x = 1/N$, where $\theta_1(x) = \sqrt{1 + 2Ax}$ and $\theta_2(x) = \sqrt{1 - 2x}$.

Proposition 7. (cf. [5, Proposition 27]) *On the assumptions in Proposition 4, if $A \geq A_0$, then $K < 240.24(A+1) + K_0$, where*

$$(A_0, K_0) \in \{(1326, 0), (454, 1000), (3, 23000), (2, 210000)\}.$$

Proof. Suppose that $K \geq 240.24(A+1)$. Applying Lemma 5 and Theorem 6 with $p_1 = A(A+1)x$, $p_2 = (A+1)y$, $q = Az$, we have

$$z^{2-\lambda} < 2C^{-1}A^{\lambda}(A+1)(A+1+2K^{-1}), \tag{3.1}$$

where $C^{-1} = 2.838 \cdot 10^{28}(A+1)N$. Since $\lambda < 2$, the assertion follows from inequality (3.1) with the inequality

$$\log z > 2m\log((A+1)K - 4), \tag{3.2}$$

which is obtained from $z = v_{2m}$ in the same way as [10, Lemma 5]. □

4. Proofs of Main Theorem and Corollary 1

Since Propositions 4 and 7 give absolute upper bounds for K and A, it remains to apply the reduction lemma ([9, Lemma 5 a)]) due to Dujella and Pethő based on [2, Lemma]. However, since the reduction method is expensive, we will apply it after making the bounds smaller.

Lemma 8. (cf. [5, Lemma 29]) *Suppose that $V_{2l} = W_{2m}$ for some integers l and m with $m \geq 2$. If $\nu = l - m$, then $\nu \geq 11$.*

Proof. Note that m can be expressed as

$$m = \left\lfloor \frac{\mu \log \beta + 0.5 \log \chi}{\log(\alpha/\beta)} \right\rfloor .$$

It can be checked by a computer that inequalities (2.5) do not hold for each ν with $1 \leq \nu \leq 10$ and for each (K, A) in the ranges obtained from Propositions 4 and 7. □

Proposition 9. (cf. [5, Proposition 30]) *On the assumptions in Proposition 4, we have $A \leq 2796$ and $K < 240.24(A+1) + 740$.*

Proof. Inequality (2.7) with $\nu \geq 11$ implies $A \leq 2796$. The other inequality $K < 240.24(A+1) + 740$ follows from (3.1), (3.2) and Lemma 2 with $\nu \geq 11$. □

Proof of Main Theorem (in the case where $\varepsilon = -2$). Applying Matveev's theorem (cf. [18]) to the linear form Λ in three logarithms, one can obtain $m < 3.4 \cdot 10^{16}$. Starting with this upper bound, we can reduce m by applying the reduction method for each K and A in the ranges obtained in Proposition 9 to get a contradiction. □

Proof of Corollary 1. Note that it always holds $r^2 \equiv \tau^2 \pmod{a}$, which proves the last assertion. Assume that $r \equiv \pm\tau \pmod{a}$ and put $r = ka \pm \tau$. Then, $b = k^2 a \pm 2\tau k$ and $c = (k+1)^2 a \pm 2\tau(k+1)$. Substituting $K = a$, $A = k$ and $\varepsilon = \pm\tau$, we see that the assertion follows from Main Theorem. □

References

[1] J. Arkin, V. E. Hoggatt, E. G. Strauss, *On Euler's solution of a problem of Diophantus*, Fibonacci Quart. **17** (1979), 333–339.

[2] A. Baker, 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.

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

[4] M. Cipu, A. Filipin, Y. Fujita, *Bounds for Diophantine quintuples II*, Publ. Math. Debrecen **88** (2016), 59–78.

[5] M. Cipu, Y. Fujita, M. Mignotte, *Two-parameter families of uniquely extendable Diophantine triples*, to appear in Sci. China Math.

[6] A. Dujella, *An absolute bound for the size of Diophantine m-tuples*, J. Number Theory **89** (2001), 126–150.

[7] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. **566** (2004), 183–224.

[8] A. Dujella, *Diophantine m-tuples*, http://web.math.pmf.unizg.hr/~duje/dtuples.html.

[9] A. Dujella, A. Pethő, *A generalization of a theorem of Baker and Davenport*, Quart. J. Math. Oxford Ser. (2) **49** (1998), 291–306.

[10] A. Filipin, B. He, A. Togbé, *On a family of two-parametric $D(4)$-triples*, Glas. Mat. Ser. III **47** (2012), 31–51.

[11] Y. Fujita, *Any Diophantine quintuple contains a regular Diophantine quadruple*, J. Number Theory **129** (2009), 1678–1697.
[12] P. E. Gibbs, Computer Bulletin **17** (1978), 16.
[13] B. He, A. Togbé, *On a family of Diophantine triples* $\{k, A^2k + 2A, (A + 1)^2k + 2(A + 1)\}$ *with two parameters*, Acta Math. Hungar. **124** (2009), 99–113.
[14] B. He, A. Togbé, *On a family of Diophantine triples* $\{k, A^2k + 2A, (A + 1)^2k + 2(A + 1)\}$ *with two parameters II*, Period. Math. Hungar. **64** (2012), 1–10.
[15] B. He, A. Togbé, V. Ziegler, *There is no Diophantine quintuple*, Preprint (2016), arXiv: 1610.04020v1.
[16] B. W. Jones, *A second variation on a problem of Diophantus and Davenport*, Fibonacci Quart. **16** (1978), 155–165.
[17] M. Laurent, *Linear forms in two logarithms and interpolation determinants II*, Acta Arith. **133** (2008), 325–348.
[18] E. M. Matveev, *An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II*, Izv. Ross. Akad. Nauk Ser. Mat. **64** (2000), 125–180. English transl. in Izv. Math. **64** (2000), 1217–1269.
[19] J. H. Rickert, *Simultaneous rational approximation and related Diophantine equations*, Math. Proc. Cambridge Philos. Soc. **113** (1993), 461–472.

Simion Stoilow Institute of Mathematics of the Romanian Academy, Research unit nr. 5, P.O. Box 1-764, RO-014700 Bucharest, Romania

Department of Mathematics, College of Industrial Technology, Nihon University, 2-11-1 Shin-ei, Narashino, Chiba, Japan

Département de Mathématique, Université de Strasbourg, 67084 Strasbourg, France