A NOTE ON DUJELLA'S UNICITY CONJECTURE

MAOHUA LE AND ANITHA SRINIVASAN

ABSTRACT. Using properties of binary quadratic Diophantine equations, we prove that if $r = p^m q^n$, where p, q are distinct odd primes and m, n are positive integers, then the equation $x^2 - \left(r^2+1\right) y^2 = r^2$ has at most one positive integer solution (x, y) with $y < r - 1$.

AMS Subject Classification: 11D09, 11R29, 11E16. Keywords: binary quadratic forms, Quadratic diophantine equation, Dujella's conjecture.

1. INTRODUCTION

Let r be a positive integer with $r \geq 2$. A. Dujella put forward the following conjecture.

Conjecture 1.1 (Dujella)**.** The equation

$$x^2 - \left(r^2+1\right) y^2 = r^2, x, y \in \mathbb{Z} \tag{1.1}$$

has at most one positive integer solution (x, y) with

$$0 < y < r - 1.$$

The above conjecture is also called Dujella's unicity conjecture, and it is related to some classical problems in number theory (see [5]). It is rather a difficult problem, and so far only the following cases have been verified. A. Filipin, Y. Fujita and M. Mignotte [2] proved the conjecture in the case when $r = p^m$, $2p^m$ or $r^2 + 1 = p, 2p^m$, where p

is an odd prime and m is a positive integer. In the case when $r = 2p^{2i}$ with p an odd prime, there is an exceptional solution $(2p^{3i} + p^i, p^i)$. The reader can find more details on exceptional solutions in [5]. A. Srinivasan [9] showed that the conjecture is true when $r = pq$, where p and q are distinct odd primes. We extend this result in our main theorem given below.

Theorem 1.2. *If $r = p^m q^n$, where p, q are distinct odd primes and $m, n \in \mathbb{N}$, then Conjecture 1.1 is true.*

Note that equation (1.1) has solutions $(r, 0)$ and $(r^2 - r + 1, r - 1)$. Our approach uses the theory of equivalence of solutions of (1.1). Each equivalence class has a unique fundamental solution (a, b) that satisfies $0 \leq b < r$. Therefore Dujella's conjecture claims that there is at most one positive fundamental solution (a, b) with $b > 0$ other than the one given above.

2. Binary quadratic forms

In this section we present the basic theory of binary quadratic forms. An excellent reference is [7], in Sections 4 to 7 and 11 of Chapter 6.

A *primitive binary quadratic form* $F = (a, b, c)$ of discriminant Δ is a function $F(x, y) = ax^2 + bxy + cy^2$, where a, b, c are integers with $b^2 - 4ac = \Delta$ and $\gcd(a, b, c) = 1$. Note that the integers b and Δ have the same parity. All forms considered here are primitive binary quadratic forms and henceforth we shall refer to them simply as forms.

Two forms F and F' are said to be (properly) *equivalent*, written as $F \sim F'$, if for some $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$ (called a transformation matrix), we have $F'(x, y) = f(\alpha x + \beta y, \gamma x + \delta y) = (a', b', c')$, where a', b', c' are given by

$$a' = F(\alpha, \gamma), \;\; b' = 2(a\alpha\beta + c\gamma\delta) + b(\alpha\delta + \beta\gamma), \;\; c' = f(\beta, \delta). \tag{2.1}$$

It is easy to see that $\sim$ is an equivalence relation on the set of forms of discriminant Δ. The equivalence classes form an abelian group called the *class group* with group law given by composition of forms. The *identity form* is defined as the form $(1, 0, \frac{-\Delta}{4})$ or $(1, 1, \frac{1-\Delta}{4})$, depending on whether Δ is even or odd respectively. The *inverse* of $F = (a, b, c)$ denoted by F^{-1}, is given by $(a, -b, c)$. In the following definition we present the formula for composition of forms.

Let $F_1 = (a_1, b_1, c_1)$ and $F_2 = (a_2, b_2, c_2)$ be two binary quadratic forms of discriminant Δ.

Definition 2.1 (Composition)**.** Let $l = gcd(a_1, a_2, (b_1 + b_2)/2)$ and let v_1, v_2, w be integers such that

$$v_1 a_1 + v_2 a_2 + w(b_1 + b_2)/2 = l.$$

If we define a_3 and b_3 as

$$a_3 = \frac{a_1 a_2}{l^2},$$
$$b_3 = b_2 + 2\,\frac{a_2}{l}\left(\frac{b_1 - b_2}{2}\; v_2 - c_2 w\right),$$

then the composition of the forms (a_1, b_1, c_1) and (a_2, b_2, c_2) is the form (a_3, b_3, c_3), where c_3 is computed using the discriminant equation.

Note that this gives the multiplication in the class group.

A form F is said to represent an integer N if there exist integers x and y such that $F(x, y) = N$. If $\gcd(x, y) = 1$, we call the representation a primitive one. Observe that equivalent forms primitively represent the same set of integers, as do a form and its inverse. Note also that if F and G are in the identity class, then so are F^{-1} and FG.

We end this section with two elementary observations about forms. Firstly, a form F represents primitively an integer N if and only if $F \sim (N, b, c)$ for some integers b, c. This follows simply by noting that $F(\alpha, \gamma) = N$ with $\gcd(\alpha, \gamma) = 1$ if and only if there exists a transformation matrix A as given above such that (2.1) holds. Secondly, if $b \equiv b' \pmod{2N}$, then the forms (N, b, c) and (N, b', c') are equivalent. This equivalence follows using the transformation matrix $A = \begin{pmatrix} 1 & \delta \\ 0 & 1 \end{pmatrix}$ where $b' = b + 2N\delta$.

3. The diophantine equation $x^2 - Dy^2 = N$

Let D be a non-square positive integer, and let N be an odd positive integer with $N > 1$ and $\gcd(D, N) = 1$. It is well known that the solutions (x, y) of the equation

$$x^2 - Dy^2 = N, \tag{3.1}$$

can be put into equivalence classes, where equivalence of solutions is defined as follows.

Definition 3.1. Two solutions (x, y) and (x', y') of $x^2 - Dy^2 = N$ are said to be equivalent, written as $(x, y) \sim (x', y')$ if $xy' \equiv yx' \pmod{N}$.

Remark 3.2. The equivalence stated above is usually stated with the additional condition of $xx' \equiv Dyy' \pmod{N}$. However, this condition follows from the congruence given in the definition.

The following lemma connects primitive representations of $x^2 - Dy^2 = N$ and forms that represent N. It is well known and one may refer to [1, Theorem 4.4, Page 53]. A clear and explicit exposition is also available in [3] and [4].

Theorem 3.3. *Let D be a non-square integer. Let $N > 1$ be a positive integer such that $\gcd(N, 2D) = 1$ and suppose that N is primitively represented by some form of discriminant $4D$. Then the following hold, where all forms are of discriminant $4D$.*

1. *If $A = \{(N, b, c) : -N < b < N\}$ and $w(N)$ is the number of distinct primes dividing N, then $|A| = 2^{w(N)}$.*
2. *There is a one-to-one correspondence between the set of equivalence classes of primitive solutions (x, y) of the equation $X^2 - DY^2 = N$ and the set $A_0 = \{(N, b, c) \sim (1, 0, -D); -N < b < N\}$ of forms in A equivalent to the identity form.*

Furthermore, in each equivalence class there is a unique fundamental solution (u, v) with least non-negative value of v. The following result gives us an upper bound for v.

Theorem 3.4. [6, Theorem 4.1] *Let $N > 1$ be an integer. Suppose that (x_0, y_0) is the least positive solution of the Pell equation $x^2 - Dy^2 = 1$. Then a solution (u, v) with $v > 0$ of $x^2 - Dy^2 = N$ is a fundamental solution if and only if either $0 < v < y_0\sqrt{N/(2(x_0+1))}$ or $v = y_0\sqrt{N/(2(x_0+1))}$ and $u = \sqrt{N(x_0+1)/2}$.*

Corollary 3.5. *Let $\gcd(a, b) = g$ with $b > 0$. Then the following are true.*

(1) *(a, b) is a fundamental solution of $x^2 - (1 + r^2)y^2 = r^2$ if and only if $b < r$.*
(2) *(a, b) is a fundamental solution of $X^2 - (1 + r^2)Y^2 = r^2$ if and only $(a/g, b/g)$ is a primitive fundamental solution of $X^2 - dY^2 = (r/g)^2$.*

Proof. The fundamental solution of the Pell equation $x^2-(1+r^2)y^2 = 1$ is $(x_0, y_0) = (2r^2 + 1, 2r)$. Using these values along with $N = r^2$ in Theorem 3.4 we obtain that a positive solution (u, v) of $x^2-(1+r^2)y^2 = r^2$ is a fundamental solution if and only if $0 < v < r$.

For part 2 we simply note that for the second equation, the upper bound in the theorem (using $N = (r/g)^2$) is r/g. □

Remark 3.6. From Theorem 3.4 we may re-word Dujella's conjecture to state that equation (1.1) has at most one positive fundamental solution (x, y) with $0 < y < r - 1$.

Lemma 3.7. [8, Lemma 3.3] *Let $k = ff'$ be a positive integer such that $1 < f < k$. If $x^2 - (k^2 + 1)y^2 = f'^2$ for some coprime integers x and y, then f' is not an odd prime power.*

Lemma 3.8. [8, Lemma 3.2] *Let $d = 1 + r^2$ and N be an integer such that $1 < |N| \leq r$. Then there are no primitive solutions to $X^2 - dY^2 = N$.*

4. Proof of Theorem 1.2

The proof of Theorem 1.2 is based on the following lemma.

Lemma 4.1. *Let $d = 1 + r^2$, with $r = p^m q^n$, where p and q are odd primes, and m and n are positive integers. Then the following are true.*

(1) *The congruence $x^2 \equiv d \pmod{pq}$ has exactly 4 solutions, namely ± 1 and $\pm l_2$, for an l_2 that satisfies $1 < l_2 < pq$.*
(2) *Let f_1, f_2, g_1, g_2 be integers such that $0 < f_1 < f_2 \leq m$ and $0 < g_1, g_2 \leq n$. Suppose that there are two forms $F = (p^{2f_1}q^{2g_1}, 2L_1, c_1)$ and $G = (p^{2f_2}q^{2g_2}, 2L_2, c_2)$ equivalent to $(1, 0, -d)$ such that $L_1 \equiv \pm L_2 \equiv \pm l_2 \pmod{pq}$. Then $g_1 > g_2$. Moreover $L_1 \equiv \pm L_2 \pmod{p^{2f_1}q^{2g_2}}$.*

Proof. The first part is a standard result from elementary number theory.

For the second part assume first that $L_2 \equiv -L_1 \pmod{pq}$. From the discriminant equation we have

$$L_2^2 \equiv L_1^2 \equiv d \pmod{\gcd(p^{2f_1}q^{2g_1}, p^{2f_2}q^{2g_2})}, \tag{4.1}$$

and as $L_2 \equiv -L_1 \pmod{pq}$, this gives

$$L_1 \equiv -L_2 \pmod{\gcd(p^{2f_1}q^{2g_1}, p^{2f_2}q^{2g_2})}. \tag{4.2}$$

We now apply the composition algorithm to find FG. If $g_1 \leq g_2$ we see that the gcd l required in Definition 2.1 is $p^{2f_1}q^{2g_1}$. Hence the first coefficient of the composition FG is $p^{2(f_2-f_1)}q^{2(g_2-g_1)}$. Therefore there is a primitive representation (x, y) such that $x^2-dy^2 = p^{2(f_2-f_1)}q^{2(g_2-g_1)} > r$ from Lemma 3.8. It follows on using Lemma 3.8 again for $p^{2f_1}q^{2g_1}$ that

$$r^2 \geq p^{2f_2}q^{2g_2} > p^{2f_1}q^{2g_1}r > r^2$$

a contradiction. Therefore we have $g_2 < g_1$, in which case from (4.2) we have $L_1 \equiv -L_2 \pmod{p^{2f_1}q^{2g_2}}$.

In the case when $L_2 \equiv L_1 \pmod{pq}$ we would proceed exactly as above with the only difference that we would now consider the composition FG^{-1}, so as to obtain the same gcd in Definition 2.1 as above. □

Proof of Theorem 1.2

We start with the observation that if $y > 0$ and $s = \gcd(x, y)$, then from Corollary 3.5(2), we have (x, y) is a fundamental solution of $X^2 - dY^2 = r^2$ if and only if $(x/s, y/s)$ is a fundamental *primitive* solution of $X^2-dY^2 = (r/s)^2$. Moreover, from Lemma 3.7 we have r/s is not a prime power. Observe that if (x, y) is a fundamental solution, then so is $(-x, y)$ and these correspond to inverse classes. Therefore it follows from Theorem 3.3 that every such pair of fundamental solutions of $x^2 - dy^2 = r^2$ corresponds to a pair of forms $(p^{2f}q^{2g}, \pm 2L, C)$, where

$$0 < f \leq m, 0 < g \leq n \text{ and } 0 < L < p^{2f}q^{2g}. \tag{4.3}$$

Note that the fundamental solutions $(\pm(r^2-r+1), r-1)$ correspond to the forms $(r^2, \pm 2, -1)$.

From Remark 3.6 to prove Dujella's conjecture, we may assume on the contrary, that there are two positive fundamental solutions different from the one mentioned above. It follows from the discussion above that we have the forms

$$F = (p^{2f}q^{2g}, 2L, C), \;\; G = (p^{2f'}q^{2g'}, 2L', C'),$$

where L and L' satisfy condition (4.3) (where in the case of L' we replace f, g, L by f', g', L' respectively) and thus

$$F \neq G \text{ or } G^{-1}.$$

From the discriminant equation we have

$$L^2 \equiv d \equiv 1 \pmod{p^{2f}q^{2g}}. \tag{4.4}$$

From Lemma 4.1(1), we have $L \equiv \pm 1$ or $\pm l_2 \pmod{pq}$. If $L \equiv \pm 1 \pmod{pq}$, then from (4.4) above we have $L \equiv \pm 1 \pmod{p^{2f}q^{2g}}$ which means

$$(p^{2f}q^{2g}, 2L, C) \sim (p^{2f}q^{2g}, \pm 2, -p^{2m-2f}q^{2n-2g}) \sim (1, 0, -d),$$

where we have used the remark at the end of Section 2. Thus $(1, 0, -d)$ represents primitively both $p^{2f}q^{2g}$ and $-p^{2m-2f}q^{2n-2g}$ (see last paragraph of Section 2). This is not possible from Lemma 3.8, if both these integers are greater than 1 in absolute value, as at least one of them is less than or equal to r in absolute value. Hence we must have $(f, g) = (m, n)$ and thus $F = (r^2, 2, -1)$ which is contrary to the assumption.

An identical analysis with L' yields

$$L \equiv \pm L' \equiv \pm l_2 \pmod{pq}. \tag{4.5}$$

If $(f, g) = (f', g')$ then the discriminant equation gives

$$L^2 \equiv L'^2 \equiv 1 \pmod{p^{2f} q^{2g}}.$$

Combining the above with (4.5) yields

$$L \equiv \pm L' \pmod{p^{2f} q^{2g}},$$

which is not possible because as stated above, $F \neq G$ or G^{-1} because of the conditions on L and L'.

Hence we may assume that $f < f'$. Then from Lemma 4.1(2) we have $g' < g$ and

$$L' \equiv -\lambda_1 L \pmod{p^{2f} q^{2g'}},$$

where $\lambda_1 = 1$ or -1. We will now compute the composition form FG^{λ_1}. We have for the gcd l in Definition 2.1

$$\gcd(p^{2f} q^{2g}, p^{2f'} q^{2g'}, L + \lambda_1 L') = p^{2f} q^{2g'}.$$

It follows from Definition 2.1 that

$$FG^{\lambda_1} = (p^{2(f'-f)} q^{2(g-g')}, 2L_1, C_1),$$

for some integers L_1, C_1. If now $g - g' \leq g'$, (i.e. $g \leq 2g'$) then we have a contradiction from Lemma 4.1(2), as $f' - f < f'$. Assume now that

$g - g' > g'$. Let $L' \equiv -\lambda_2 L_1 \pmod{pq}$. Then

$$FG^{\lambda_1+\lambda_2} = (p^{2f}q^{2(g-2g')}, 2L_2, C_2),$$

where the required gcd in Definition 2.1 is $l = p^{2(f'-f)}q^{2g'}$. Observe that the exponent of p in the form displayed above is $2f$ (the same as in F) and the exponent of q is less than the corresponding exponent in F, which is not possible by Lemma 4.1, and thus the proof is complete.

Acknowledgement

We are grateful to the referee for an extremely careful reading of the manuscript, making it mathematically and technically more precise.

References

[1] D. A. Buell, *Binary Quadratic Forms, Classical Theory and Modern Computations,*Springer-Verlag, New York, 1989.

[2] A. Filipin, Y. Fujita, M. Mignotte, *The non extendibility of some parametric families of $D(-1)$- triples*, Quart. J. Math, 2012, **63**, 605–621.

[3] Y. Fujita, M.-H. Le, *Some exponential Diophantine equations II: The equation $x^2 - Dy^2 = k^z$ for even k*, Math. Slovaca, 2022, **72** (2), 341–354.

[4] M.-H. Le, *Some exponential Diophantine equations I: The equation $D_1x^2 - D_2y^2 = \lambda k^z$*, J. Number Theory, 1995, **55**, 209–221.

[5] K. Matthews, J. Robertson and J. White, *On a diophantine equation of Andrej Dujella*, Glas. Mat. Ser. III, **48** (2013), 265–289.

[6] K. Matthews, J. Robertson and A. Srinivasan, *On fundamental solutions of binary quadratic form equations,* Acta Arithmetica, 2015, **169** (3).

[7] P. Ribenboim, *My Numbers, My Friends, Popular Lectures on Number Theory*, Springer-Verlag, 2000.

[8] A. Srinivasan, *On the prime divisors of elements of a $D(-1)$ quadruple*, Glas. Mat. Ser. III,2014, **49**(2), 275–285.

[9] A. Srinivasan, *$D(-1)$ quadruples and products of two primes*, Glas. Mat. Ser. III,2015, **50**(2), 261–268.

Institute of Mathematics, Lingnan Normal College, Zhangjiang, Guangdong, 524048, China

E-mail address: lemaohua2008@163.com

Departamento de métodos cuantitativos, Universidad Pontificia de Comillas (ICADE), C/ Alberto Aguilera, 23 - 28015 Madrid

E-mail address: asrinivasan@icade.comillas.edu