GLASNIK MATEMATIČKI
Vol. 50(70)(2015), 261 – 268

$D(-1)$-QUADRUPLES AND PRODUCTS OF TWO PRIMES

Anitha Srinivasan
Saint Louis University-Madrid campus, Spain

Abstract. A $D(-1)$-quadruple is a set of positive integers $\{a,b,c,d\}$, with $a<b<c<d$, such that the product of any two elements from this set is of the form $1+n^2$ for some integer n. Dujella and Fuchs showed that any such $D(-1)$-quadruple satisfies $a=1$. The $D(-1)$ conjecture states that there is no $D(-1)$-quadruple. If $b=1+r^2, c=1+s^2$ and $d=1+t^2$, then it is known that r,s,t,b,c and d are not of the form p^k or $2p^k$, where p is an odd prime and k is a positive integer. In the case of two primes, we prove that if $r=pq$ and v and w are integers such that $p^2v-q^2w=1$, then $4vw-1>r$. A particular instance yields the result that if $r=p(p+2)$ is a product of twin primes, where $p\equiv 1 \pmod 4$, then the $D(-1)$-pair $\{1,1+r^2\}$ cannot be extended to a $D(-1)$-quadruple. Dujella's conjecture states that there is at most one solution (x,y) in positive integers with $y<k-1$ to the diophantine equation $x^2-(1+k^2)y^2=k^2$. We show that the Dujella conjecture is true when k is a product of two odd primes. As a consequence it follows that if t is a product of two odd primes, then there is no $D(-1)$-quadruple $\{1,b,c,d\}$ with $d=1+t^2$.

1. Introduction

Let n be a nonzero integer. A diophantine m-tuple with the property $D(n)$, is a set of m positive integers, such that if a,b are any two elements from this set, then $ab+n=k^2$ for some integer k. We will look at the case $n=-1$. The cases $n=1$ and $n=4$ have been studied in great detail and still continue to be areas of active research. For more details on this subject the reader may consult [1], where a comprehensive and up to date list of references is available.

2010 *Mathematics Subject Classification.* 11D09, 11R29, 11E16.
Key words and phrases. Diophantine m–tuples, binary quadratic forms, quadratic diophantine equation.

In the case of $n = -1$, it has been conjectured that there is no $D(-1)$-quadruple. The first significant progress was made by Dujella and Fuchs ([2]), who showed that if $\{a, b, c, d\}$ is a $D(-1)$-quadruple with $a < b < c < d$, then $a = 1$. Subsequently, Dujella et. al. ([3]) proved that there are only a finite number of such quadruples. Filipin and Fujita ([4]) showed that if $\{1, b, c\}$ is $D(-1)$-triple with $b < c$, then there exist at most two d's such that $\{1, b, c, d\}$ is a $D(-1)$-quadruple.

Filipin, Fujita and Mignotte ([5]) showed that if $b = r^2 + 1$, then in each of the cases $r = p^k$, $r = 2p^k$, $b = p$ and $b = 2p^k$, where p is an odd prime and k is a positive integer, the $D(-1)$-pair $\{1, b\}$ cannot be extended to a $D(-1)$-quadruple $\{1, b, c, d\}$ with $b < c < d$. In [13] we showed that this also holds for $c = 1 + s^2$, that is, if $s = p^k$, $s = 2p^k$, $c = p$ or $c = 2p^k$, then the $D(-1)$-triple $\{1, b, c\}$ cannot be extended to a $D(-1)$-quadruple (one of the referees pointed out that this result was essentially proved in [5]). It is also known that the results mentioned above for b and c also hold for $d = 1 + t^2$ (see discussion following Conjecture 1.3). Note that b, c and d cannot be of the form p^k with $k > 1$ and p prime (see [8]). In the case of a product of two primes, we showed in [13] that if $r = pq$ then $p^4, q^4 > r$. The following result gives further conditions in this case.

THEOREM 1.1. *Let* $\{1, b, c, d\}$ *with* $1 < b < c < d$ *be a* $D(-1)$*-quadruple with* $b = 1+r^2$ *where* $r > 0$*. Let* $r = pq$*, where* p *and* q *are distinct odd primes, and let* v *and* w *be integers such that* $p^2v - q^2w = 1$*. Then* $4vw - 1 > r$*.*

COROLLARY 1.2. *Let* $b = 1 + r^2$ *and* $r = p(p + 2)$ *where* p *and* $p + 2$ *are both primes and* $p \equiv 1 \pmod 4$*. Then the* $D(-1)$*-pair* $\{1, b\}$ *cannot be extended to a* $D(-1)$*-quadruple.*

The following conjecture made by Andrej Dujella is closely related to the $D(-1)$ conjecture.

CONJECTURE 1.3. (Andrej Dujella) *Let* $k \geq 2$*. Then there exists at most one solution* (x, y) *in positive integers to the equation* $x^2 - (k^2 + 1)y^2 = k^2$ *with* $y < k - 1$*.*

In [9] the authors studied the equation $x^2 - (k^2 + 1)y^2 = k^2$, calling it the Dujella equation and the conjecture above, which they called the unicity conjecture. They used a continued fraction approach and gave some interesting equivalent conjectures.

It is known that Dujella's unicity conjecture implies the $D(-1)$ conjecture (see [9, Section 17]). Indeed the result [5] on the $D(-1)$ conjecture mentioned above, is based on [5, Lemma 6.1], which states that Conjecture 1.3 is true for the same cases, namely, when $k^2 + 1 = p, 2p^n$, or $k = p^n, 2p^n$, where p is an odd prime and n is a positive integer. It follows, also from [5, Lemma 6.1], that the $D(-1)$ conjecture holds in the case when t or $d = 1 + t^2$ is of the form p^n or $2p^n$, where p is an odd prime and k is a positive integer.

K. Matthews communicated to the author an unpublished short proof (along with J. Robertson) of Conjecture 1.3 in the case when k^2+1 is divisible by exactly two odd primes. We show that Conjecture 1.3 is true when k is a product of two odd primes.

THEOREM 1.4. *Let $k = pq$ where p and q are distinct odd primes. Then the equation $x^2 - (1+k^2)y^2 = k^2$ has at most one solution (x, y) in positive integers with $y < k-1$.*

An immediate corollary is the following.

COROLLARY 1.5. *If x is a product of two distinct odd primes and $d = 1+x^2$, then there is no $D(-1)$-quadruple $\{1, b, c, d\}$ with $1 < b < c < d$.*

2. Binary quadratic forms

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

A *primitive binary quadratic form* $f = (a, b, c)$ of discriminant d is a function $f(x, y) = ax^2 + bxy + cy^2$, where a, b, c are integers with $b^2 - 4ac = d$ and $\gcd(a, b, c) = 1$. Note that the integers b and d 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 *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

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

It is easy to see that $\sim$ is an equivalence relation on the set of forms of discriminant d. 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 $(1, 0, \frac{-d}{4})$ or $(1, 1, \frac{1-d}{4})$, depending on whether d is even or odd respectively. The *inverse* of $f = (a, b, c)$ denoted by f^{-1}, is given by $(a, -b, c)$.

A form f is said to represent an integer m if there exist integers x and y such that $f(x, y) = m$. 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. Hence, sometimes we will refer to a class of forms that represents an integer.

We end this section with two elementary observations about forms. Firstly, if a form f represents primitively an integer n, then $f \sim (n, b, c)$ for some integers b, c. This follows simply by noting that if $f(\alpha, \gamma) = n$ with $\gcd(\alpha, \gamma) = 1$, then 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 $x^2 - dy^2 = n$

For any positive integer d that is not a square, all representations (x, y) of an integer n by the form $(1, 0, -d)$ may be put into equivalence classes using the following notion of equivalence.

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 the following congruences*

$$xx' \equiv dyy' \pmod{n}, \quad xy' \equiv yx' \pmod{n} \tag{3.1}$$

are satisfied.

The result given below is used at several places, and hence we isolate it as a lemma.

Lemma 3.2. *Let k be an odd integer. If a solution (x, y) of the equation $x^2 - (1 + k^2)y^2 = k^2$ satisfies $(x, y) \sim (x, -y)$, then k divides x and y.*

Proof. If $(x, y) \sim (x, -y)$, then (3.1) gives $x^2 \equiv -y^2 \pmod{k^2}$. Moreover, from the Dujella equation, $x^2 \equiv y^2 \pmod{k^2}$, hence k divides x and y. ∎

The following lemma connects primitive representations of $x^2 - dy^2 = n$ and forms that represent n and is crucial for our proofs.

Lemma 3.3. *Let n be a positive integer such that $\gcd(n, 2\Delta) = 1$ and suppose that n is primitively represented by some form of discriminant Δ. Then the following claims hold.*

1. *If $A = \{(n, b, c); 0 < b < 2n\}$ 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 $A_0 = \{(n, b, c) \sim (1, 0, -d); 0 < b < 2n\}$ of forms in A equivalent to the identity form.*

Proof. As n is primitively represented by some form of discriminant Δ, there is a solution to the congruence $\Delta \equiv x^2 \pmod{4n}$ ([11, Solution of problem 1]). It follows from a classical result (see for instance [14, Chapter V, §4] or [7, Theorem 122]) that there are $2^{w(n)+1}$ solutions modulo $4n$. As x and $-x$ are both solutions to $\Delta \equiv x^2 \pmod{4n}$, there are $2^{w(n)}$ solutions to the congruence $\Delta \equiv x^2 \pmod{4n}$ with $0 < x < 2n$. The first part of the lemma now follows from [11, Solution of problem 2], where it is shown that there is a one-to-one correspondence between the set A and solutions to the congruence $\Delta \equiv x^2 \pmod{4n}$ with $0 < x < 2n$.

The second part of the lemma follows from the following facts that are given in [11, Solution of problem 3]. Each primitive representation (x, y) of $X^2 - dY^2 = n$ corresponds to a unique form (n, b, c), where $0 < b < 2n$. If two such representations correspond to the same form, then the representations are equivalent. Moreover, each form in set A_0 corresponds to a unique equivalence class of primitive representations (x, y) of $X^2 - dY^2 = n$, and hence the correspondence in part 2 of the lemma follows. ∎

The next lemma has been used by several authors in the study of the current problem, such as [5, Lemma 6.2] and [13, Lemma 3.2].

LEMMA 3.4 ([6, Lemma 2.3]). *Let n be an integer such that $1 < |n| \leq k$. Then there are no primitive solutions (x, y) such that $x^2 - (k^2 + 1)y^2 = n$.*

A useful consequence of the above lemma is the following result.

LEMMA 3.5 ([13, 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.*

4. PROOFS

Throughout this section the following terminology will be used.

Let $\{1, b, c, d\}$ be a $D(-1)-$quadruple with $1 < b < c < d$. Set

$$b = 1 + r^2, \quad c = 1 + s^2, \quad d = 1 + x^2$$

and

$$bd = 1 + y^2, \quad cd = 1 + z^2, \quad bc = 1 + t^2.$$

Then

$$t^2 - (1 + r^2)s^2 = r^2 \tag{4.1}$$

and

$$t^2 - (1 + s^2)r^2 = s^2. \tag{4.2}$$

It is easy to see (using (3.1)) that the equation $X^2 - (r^2 + 1)Y^2 = r^2$ has the inequivalent solutions $(r, 0)$ and $(r^2 + 1 - r, \pm(r - 1))$. In [5], solutions equivalent to these three solutions were called regular solutions and it was shown that (t, s) is not a regular solution.

LEMMA 4.1 ([5, Corollary 1.2]). *The solution (t, s) of $X^2 - bY^2 = r^2$ is not equivalent to any of the solutions $(b - r, \pm(r - 1))$ and $(r, 0)$.*

LEMMA 4.2. *Let $r = pq$ where p and q are distinct odd primes. Then there are exactly four inequivalent classes of primitive representations of r^2 by the form $(1, 0, -(1 + r^2))$, namely, $(b - r, \pm(r - 1))$ and $(t, \pm s)$. Moreover, r^2 is primitively represented only by the identity class.*

Proof. Let $\gcd(t,s)=n$. As $r=pq$, from (4.1) we have $n=1,r,p$ or q. Observe that by Lemma 3.5 the cases $n=p$ and $n=q$ are not possible. If $n=r$, then t and s are divisible by r. It follows by equivalence of solutions (Definition 3.1) that $(t,s)\sim(r,0)$, which is not possible by Lemma 4.1. Hence $\gcd(t,s)=1$, and it follows from Lemma 3.2 and Lemma 4.1 that $(b-r,\pm(r-1))$ and $(t,\pm s)$ are inequivalent primitive representations. By Lemma 3.3, the set A_0 (given therein) has at least 4 elements. Moreover, by the same lemma, the set A has exactly 4 elements and therefore $A=A_0$ as $A_0\subseteq A$ and hence there are exactly four inequivalent classes of primitive representations of r^2 by $(1,0,-b)$, namely the ones given above. □

The second part of the following lemma follows on application of [12, Theorem 1] (a converse to Nagell's theorem). However, the article mentioned above only provides an outline of the proof and we are grateful to a referee for the details given below.

Lemma 4.3. *Let $k=pq$, where p and q are distinct odd primes. Then the following hold.*

1. *Any solution (α,β) of $X^2-(1+k^2)Y^2=k^2$ with $0<\beta<k$ satisfies $\gcd(\alpha,\beta)=1$.*
2. *Let (x,y) and (x',y') be two equivalent solutions in positive integers to $X^2-(1+k^2)Y^2=k^2$ that satisfy $y,y'<k-1$. Then $x=x'$ and $y=y'$.*

Proof. As seen in the beginning of the proof of Lemma 4.2, either $\gcd(\alpha,\beta)=1$ or k divides both α and β, the latter of which is not possible as $0<\beta<k$ and hence $\gcd(\alpha,\beta)=1$.

For the second part, observe that $(2k^2+1,2k)$ is the fundamental solution of the Pell equation $X^2-(1+k^2)Y^2=1$. It is well known (see for example [12]) that if (x,y) and (x',y') are equivalent, then

$$x'+y'\sqrt{d}=\pm(x+y\sqrt{d})(2k^2+1+2k\sqrt{d})^n, \tag{4.3}$$

for some integer n. Since $x^2-dy^2=k^2$, we may rewrite (4.3) as

$$(x'+y'\sqrt{d})(x-y\sqrt{d})=\pm k^2(2k^2+1+2k\sqrt{d})^n=A+B\sqrt{d}. \tag{4.4}$$

It is easy to see that $2k^3$ divides B in the above equation and hence it also divides $xy'-yx'$. Observe that since y and y' are positive integers less than $k-1$, it follows from the Dujella equation that x and x' are less than k^2-k+1. Hence, as $xy'-yx'$ is divisible by $2k^3$, we have $xy'=yx'$, which gives $x=x'$ and $y=y'$, since from part one of the lemma $\gcd(x,y)=\gcd(x',y')=1$. □

Proof of Theorem 1.1. Let v and w be integers such that $vp^2-wq^2=1$ and let h be the form $(r^2,4q^2w+2,4vw-1)$, where $r=pq$. It is straightforward to see that h is a form of discriminant $4b$ and that $4vw-1>0$. Moreover, h primitively represents r^2 and thus, by Lemma 4.2, we have $h\sim(1,0,-b)$.

Furthermore, h also primitively represents $4vw-1$ and hence, by Lemma 3.4, we have $4vw-1>r$. □

PROOF OF COROLLARY 1.2. Note that if $v=\frac{p+3}{4}$ and $w=\frac{p-1}{4}$, then we have $vp^2-w(p+2)^2=1$. Moreover, $4vw-1=(p+3)\frac{p-1}{4}-1<p(p+2)$ and the corollary follows from Theorem 1.1. □

PROOF OF THEOREM 1.4. Let (x,y) be a solution of the Dujella equation $x^2-(1+k^2)y^2=k^2$, with $x,y>0$ and $y<k-1$. Then $x=|x|<k^2-k+1$ and $0<x+y<k^2$. Now suppose that $(x,y)\sim(1+k^2-k,\pm(k-1))$. Then (3.1) gives

$$x\equiv\pm y \pmod{k^2}, \tag{4.5}$$

which is not possible, as we have shown above that $0<x+y<k^2$. Therefore (x,y) is not equivalent to either of the solutions $(1+k^2-k,\pm(k-1))$. Furthermore, using Lemma 3.2 and Lemma 4.3, part 1, it follows that the solutions $(x,\pm y)$ and $(1+k^2-k,\pm(k-1))$ are inequivalent primitive solutions. Therefore $|A_0|\geq 4$, where A_0 is as given in Lemma 3.3. From the same lemma we have $|A|=4$ and as $A_0\subseteq A$ it follows that $A_0=A$. Thus there are exactly four inequivalent classes of primitive solutions, namely the classes represented by $(x,\pm y)$ and $(1+k^2-k,\pm(k-1))$. Now, if (x',y') is another solution in positive integers to the Dujella equation satisfying $y'<k-1$, then it must be equivalent to one of $(x,\pm y)$ (since we have shown above that any such solution is not equivalent to $(1+k^2-k,\pm(k-1))$). From Lemma 4.3 part 2, we have $(x,y)=(x',y')$, and hence there is at most one solution in positive integers (x,y) with $y<k-1$ to the equation $X^2-(1+k^2)Y^2=k^2$, and the theorem is proved. □

PROOF OF COROLLARY 1.5. By Theorem 1.4, if x is a product of two distinct odd primes, then the equation $\alpha^2-(1+x^2)\beta^2=x^2$ has at most one positive solution (α,β) with $\beta<x-1$. In other words, the Dujella conjecture holds for this equation and as shown in [9, Section 17], this implies that the $D(-1)$ conjecture is true. □

ACKNOWLEDGEMENTS.

I greatly appreciate the efforts of both referees in reading the manuscript extremely carefully. Their comments helped to refine the proofs of the main theorems that are now quite neat and succinct. In particular, I am thankful to the referee for providing the proof of part 2 of Lemma 4.3, which is crucial in proving Theorem 1.4.

REFERENCES

[1] A. Dujella, Diophantine m-tuples references (chronologically), `http://web.math.pmf.unizg.hr/~duje/ref.html`.

[2] A. Dujella and C. Fuchs, *Complete solution of a problem of Diophantus and Euler*, J. London Math. Soc. **71** (2005), 33–52.
[3] A. Dujella, A. Filipin and C. Fuchs, *Effective solution of the $D(-1)$-quadruple conjecture*, Acta Arith. **128** (2007), 319–338.
[4] A. Filipin and Y. Fujita, *The number of $D(-1)$-quadruples*, Math. Commun., **15** (2010), 387–391.
[5] A. Filipin, Y. Fujita and M. Mignotte, *The non-extendibility of some parametric families of $D(-1)$-triples*, Q. J. Math. **63** (2012), 605–621.
[6] Y. Fujita, *The non-extensibility of $D(4k)$-triples $\{1, 4k(k-1), 4k^2+1\}$ with $|k|$ prime*, Glas. Mat. Ser. III **41** (2006), 205–216.
[7] G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, Fifth edition. The Clarendon Press, Oxford University Press, New York, 1979.
[8] V. A. Lebesgue, *Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$*, Nouv. Ann. Math. **9** (1850), 178–181.
[9] K. Matthews, J. Robertson and J. White, *On a diophantine equation of Andrej Dujella*, Glas. Mat. Ser. III **48** (2013), 265–289.
[10] T. Nagell, Introduction to Number Theory, Wiley, New York, 1951.
[11] P. Ribenboim, My Numbers, My Friends, Popular Lectures on Number Theory, Springer-Verlag, New York, 2000.
[12] J. Robertson, *Fundamental solutions to generalized Pell equations*, `http://www.jpr2718.org/FundSoln.pdf`
[13] A. Srinivasan, *On the prime divisors of elements of a $D(-1)$ quadruple*, Glas. Mat. Ser. III **49** (2014), 275–285.
[14] I. M. Vinogradov, Elements of number theory, Dover Publications, New York, 1954.

A. Srinivasan
Department of Mathematics
Saint Louis University-Madrid campus
Avenida del Valle 34, 28003 Madrid
Spain

Received: 10.6.2014.
Revised: 18.9.2014. & 8.10.2014.