On the prime divisors of elements of a $D(-1)$ quadruple

Anitha Srinivasan *

Abstract

In [5] it was shown that if $\{1, b, c, d\}$ is a $D(-1)$ quadruple with $b < c < d$ and $b = 1 + r^2$, then r and b are not of the form $r = p^k$, $r = 2p^k$, $b = p$ or $b = 2p^k$, where p is an odd prime and k is a positive integer. We show that an identical result holds for $c = 1 + s^2$, that is, the cases $s = p^k$, $s = 2p^k$, $c = p$ and $c = 2p^k$ do not occur for the $D(-1)$ quadruple given above. For the integer $d = 1 + x^2$, we show that d is not prime and that x is divisible by at least two distinct odd primes. Furthermore, we present several infinite families of integers b, such that the $D(-1)$ pair $\{1, b\}$ cannot be extended to a $D(-1)$ quadruple. For instance, we show that if $r = 5p$ where p is an odd prime, then the $D(-1)$ pair $\{1, r^2 + 1\}$ cannot be extended to a $D(-1)$ quadruple.

1 Introduction

Let n be a non zero 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

---

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

to be areas of active research. For more details on these cases, the reader may consult the references given in [5] or [?], where a comprehensive and up to date list of references is available.

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.

Recently, 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 $b < c < d$. The existence of a $D(-1)$ quadruple is closely related to the existence of solutions of quadratic diophantine equations of the type $X^2 - (1 + Z^2)Y^2 = Z^2$. The above result of [5] is a corollary of an extremely useful result proved therein ([5, Theorem 1.1] or Lemma 4.1 for a partial result) on the equivalence of certain solutions of the diophantine equation $X^2 - (1 + r^2)Y^2 = r^2$. We use this result in conjunction with our methods from class groups to prove our theorems. Our first theorem shows that the result in [5] mentioned above, also holds for c and d. (Note that d is known to be odd and b, c and d cannot be of the form p^k with $k > 1$ and p prime.)

Theorem 1.1. *Let $\{1, b, c, d\}$ with $1 < b < c < d$ be a $D(-1)$ quadruple where $c = 1 + s^2$. Let p be an odd prime and k a positive integer. Then the cases $c = p$, $d = p$, $c = 2p^k$, $s = p^k$ and $s = 2p^k$ do not occur. Moreover, if $d = 1 + x^2$, then x is divisible by at least two distinct odd primes.*

In the case of a product of two odd primes, we have the following result.

Theorem 1.2. *Let $\{1, b, c, d\}$ be a $D(-1)$ quadruple with $b < c < d$. If $b = 1 + r^2$ and $r = pq$, where p and q are distinct odd primes, then $p, q > r^{\frac{1}{4}}$.*

Corollary 1.3. *Suppose that α is a positive integer such that for each $r \leq \alpha$ the $D(-1)$ pair $\{1, r^2+1\}$ cannot be extended to a $D(-1)$ quadruple. Then for each odd prime $p \leq \alpha^{\frac{1}{4}}$ and any odd prime $q \neq p$, the $D(-1)$ pair $\{1, (pq)^2+1\}$ cannot be extended to a $D(-1)$ quadruple.*

Remark 1.4. *To illustrate a concrete case of the above corollary, note that one may verify that if $r \leq \alpha = 5^4$, then the $D(-1)$ pair $\{1, r^2 + 1\}$ cannot be extended to a $D(-1)$ quadruple. Hence if $p = 5$, then for $r = pq > 5^4$, we have $p = 5 = \alpha^{\frac{1}{4}}$ and therefore by Corollary 1.3 the $D(-1)$ pair $\{1, (5q)^2 + 1\}$ cannot be extended to a $D(-1)$ quadruple for any odd prime q.*

Theorem 1.5. *Let $r = P\phi$, where P is prime and $\phi < r^{\frac{1}{4}}$. Then there is no $D(-1)$ triple $\{1, r^2 + 1, s^2 + 1\}$ with $\gcd(r, s) = 1$.*

We provide an entirely new approach via the theory of binary quadratic forms and the class group to study this problem. This is possible as the existence of a $D(-1)$ triple is intimately connected to the representations of integers by certain binary quadratic forms and hence to the class group.

2 Binary quadratic forms and the class group

In this section we present the basic theory of binary quadratic forms. An excellent and delightful reference for this topic is [7], where in particular, the reader may consult Sections 4 to 7 and Section 11 for the material presented here. Other useful references are [6] and [1], where the former uses the language of ideals and the latter that of forms.

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 $\gcd(a, b, c) = 1$. We sometimes refer to the integer a as the *first coefficient* of the form f. 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 (see Definition 2.2).

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.

We put together some basic facts about forms of discriminant d in the following lemma.

Lemma 2.1. ([7, Solutions of problems 1, 2 and 3, Section 7]) *The following hold for forms of discriminant d.*

1. *An integer n is primitively represented by a form f if and only if $f \sim (n, b, c)$ for some integers b, c.*

2. *If $f = (n, b, c)$ and $f' = (n, b', c')$ are two forms such that $b \equiv b' \pmod{2n}$, then $f \sim f'$.*

3. *Let n be a positive integer such that either $n = 4$ or $\gcd(n, 2d) = 1$ and n is primitively represented by some form. If $w(n)$ is the number of distinct primes dividing n, then there are at most $2^{w(n)-1}$ pairs of classes of forms $\{f, f^{-1}\}$ that represent n.*

In the following definition we present the formula for the composition of forms that gives the group multiplication for the class group.

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 d.

Definition 2.2. Let $g = \gcd(a_1, a_2, (b_1 + b_2)/2)$ and let v_1, v_2, w be integers such that
$$v_1 a_1 + v_2 a_2 + w(b_1 + b_2)/2 = g.$$
If we define a_3 and b_3 as
$$a_3 = \frac{a_1 a_2}{g^2},$$
$$b_3 = b_2 + 2\frac{a_2}{g}\left(\frac{b_1 - b_2}{2}v_2 - c_2 w\right) \pmod{2a_3},$$
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 $b_3^2 - 4a_3 c_3 = d$. Note that b_3 is taken modulo $2a_3$ because of Lemma 2.1, part 2.

4

3 The diophantine equation $x^2 - dy^2 = n$

The study of $D(-1)$ quadruples leads to the study of forms $(1, 0, -d) = x^2 - dy^2$ of discriminant $4d$. If (x, y) is a primitive representation of an integer n by this form (i.e. $x^2 - dy^2 = n$), then there exist integers α and β such that the matrix $A = \begin{pmatrix} x & \alpha \\ y & \beta \end{pmatrix}$ has determinant 1. By (2.1) the matrix A transforms the form $(1, 0, -d)$ to a form $(n, 2b, c)$. Observe that the choice of α and β is not unique. The following facts are easy to verify (see for example [7, Solution of problem 3, Section 7]). Any choice of integers u, v, such that $xv - yu = 1$, yields a transformation matrix that takes $(1, 0, -d)$ to a form $(n, 2b', c')$ where $b' \equiv b \pmod{n}$. Moreover, it may be verified that if $(n, 2b', c') \sim (1, 0, -d)$ is a form such that $b' \equiv b \pmod{n}$, then there exist integers u, v such that $xv - yu = 1$. Therefore, for each primitive representation (x, y) of n by the form $(1, 0, -d)$, there corresponds a unique integer $b \pmod{n}$. We say in this case that the representation (x, y) belongs to b.

If two primitive representations (x, y) and (x', y') (of n by $(1, 0, -d)$) belong to the same integer b, then it may be verified that

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

We call such representations as equivalent. The congruences in (3.1) may be used to define equivalence of general solutions (that are not necessarily primitive) 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 the congruences (3.1) are satisfied.

The following lemma is easy to verify using the theory of class groups. The first part of this lemma has been used by several authors in the study of the current problem, such as [5, Lemma 6.2]. We provide a sketch of the proof to give a flavour of the elegant infrastructure of the class group of a real quadratic field.

Lemma 3.2. *Let $d = 4(1 + s^2)$ and n be an integer such that $1 < |n| \leq s$. Then the following hold.*

1. *There are no primitive solutions (x, y) such that $x^2 - (s^2 + 1)y^2 = n$.*

2. If $s = 2p^k$ and (x, y) is a primitive solution of $4x^2 + 2xy - p^{2k}y^2 = n$, then $|n| = 4$ or p^k.

Proof. The reader may refer to [1, Chapter 3] for details on cycles of forms in real quadratic fields and how to compute them. Each equivalence class in the class group is represented by a finite cycle of forms. The identity class here is represented by the cycle

$$(1, 2s, -1) \sim (-1, 2s, 1),$$

and when $s = 2p^k$, the cycle corresponding to the form $(4, 2, -p^{2k})$ is

$$(p^k, 2(p^k + 1), -3p^k + 2) \sim (-3p^k + 2, 2(2p^k - 3), 4) \sim (4, 2(2p^k - 1), -p^k) \sim$$

$$(-p^k, 2(p^k + 1), 3p^k - 2) \sim (3p^k - 2, 2(2p^k - 3), -4) \sim (-4, 2(2p^k - 1), p^k).$$

It is easy to show that if $|m| < \frac{\sqrt{d}}{2}$ and m is primitively represented by a form f, then there is a form (m, b, c) for some integers b, c that appears in the cycle representing f ([6, Corollary 1.4.3, p. 19]). Note that $|n| \leq s < \frac{\sqrt{d}}{2}$. In the first part of the lemma, n is primitively represented by the identity form $(1, 0, -(s^2 + 1))$ and in the second part, by the form $(4, 2, -p^{2k})$. Therefore, by the result mentioned above, n must appear as a first coefficient of some form in the first cycle given above for part 1 (which is not the case), and the second cycle for part 2 (which gives $|n| = 4$ or p^k). $\square$

The following result is a useful consequence of the above lemma that we use to prove our theorems.

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.*

Proof. As $x^2 - (k^2 + 1)y^2 = f'^2$, it follows from Lemma 3.2 that $f < f'$, that is $f' > \sqrt{k}$. Moreover, as $(1, 0, -(k^2 + 1))$ primitively represents f'^2, by Lemma 2.1, part 1, there is a form $(f'^2, 2b, c)$ for some integers b, c such that $(1, 0, -d) \sim (f'^2, 2b, c)$.

Observe that $(f'^2, 2, -f^2)$ is a form of discriminant $4(k^2 + 1)$. If f' is an odd prime power, then by Lemma 2.1 part 3, we have $(f'^2, 2b, c) \sim (f'^2, 2, -f^2)$ or $(f'^2, 2b, c) \sim (f'^2, -2, -f^2)$ and hence as equivalent forms primitively represent the same integers, the form $(1, 0, -d)$ primitively represents $-f^2$ (as the forms $(f'^2, \pm 2, -f^2)$ represent $-f^2$ via the representation $(0, 1)$), which is not possible by Lemma 3.2, as $f^2 < k$. $\square$

6

4 Proofs of theorems

The following terminology will hold throughout this section.

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

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

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

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

Observe that for any positive integer $k > 1$, the equation $X^2 - (k^2 + 1)Y^2 = k^2$ has the inequivalent solutions $(k, 0)$ and $(k^2 + 1 - k, \pm(k - 1))$.

Lemma 4.1. ([5, Theorem 1.1]) *The solution (t, s) given in (4.1) of $X^2 - bY^2 = r^2$ is not equivalent to any of the solutions $(b - r, \pm(r - 1))$ and $(\pm r, 0)$.*

Lemma 4.2. [4, Proof of Theorem 1, p. 389] *If $M = \operatorname{lcm}(r, s)$, then $x \equiv 0 \pmod{M^2}$.*

For the following lemma note that if (x, y) is a primitive solution of $X^2 - (k^2 + 1)Y^2 = k^2$, then $(x, y) \not\sim (x, -y)$. Note also that if the representation (x, y) belongs to the integer b, then $(x, -y)$ belongs to the integer $-b$.(See beginning of Section 3.)

Lemma 4.3. *Let k be an odd positive integer such that there are two primitive solutions (a, b) and (a', b') to $X^2 - (k^2 + 1)Y^2 = k^2$ such that $(a, b) \not\sim (a', \pm b')$. Then there exist coprime integers p, q both greater than 1, with $k = pq$ such that p^4 and q^4 are primitively represented by the form $X^2 - (k^2 + 1)Y^2$.*

Proof. The given two primitive solutions to $X^2 - (k^2 + 1)Y^2 = k^2$, by Lemma 2.1 part 1, give rise to two forms P_1 and P_2 equivalent to $(1, 0, -(k^2 + 1))$ such that $P_1 = (k^2, 2b_1, c_1)$ and $P_2 = (k^2, 2b_2, c_2)$, where b_1, b_2 satisfy $b_1 \not\equiv \pm b_2 \pmod{k^2}$ (see remark preceding this lemma). Observe that from the discriminant equation we have $b_1^2 \equiv b_2^2 \pmod{k^2}$. As $\gcd(k, b_i) = 1$, there exist coprime integers p, q greater than 1 with $k = pq$ such that

$$b_1 + b_2 \equiv 0 \pmod{p^2}, \; b_1 - b_2 \equiv 0 \pmod{q^2}. \tag{4.3}$$

7

Let $I = (p^2, 2b_1, c_1q^2)$ and $J = (q^2, 2b_1, c_1p^2)$. By Definition 2.2 (composition of forms), as p, q are coprime, we have $IJ \sim P_1$ and $I^{-1}J \sim P_2$ and hence

$$(1, 0, -(k^2 + 1)) \sim P_1 \sim IJ \sim P_2 \sim I^{-1}J.$$

It follows that

$$I \sim I^{-1} \sim J,$$

and therefore $I^2 \sim J^2 \sim (1, 0, -(k^2 + 1))$. Using Definition 2.2 again, it is easy to verify that $I^2 = (p^4, 2\phi, \psi)$ for some integers ϕ and ψ and hence, as $I^2 \sim (1, 0, -(k^2 + 1))$, the form $(1, 0, -(k^2 + 1))$ primitively represents p^4. Similarly $(1, 0, -(k^2 + 1))$ also primitively represents q^4. $\qquad\square$

Proof of Theorem 1.1 Suppose that $c = p$ for some odd prime p. From (4.1) we have

$$t^2 - s^2 = r^2(1 + s^2) \tag{4.4}$$

so that for some decomposition $r = r_1r_2$ we have

$$\frac{t - s}{r_1^2} \frac{t + s}{r_2^2} = 1 + s^2 = p.$$

Therefore either

$$t - s = pr_1^2, \quad t + s = r_2^2 \tag{4.5}$$

or

$$t - s = r_1^2, \quad t + s = pr_2^2. \tag{4.6}$$

In the case of (4.5) we have

$$2s + cr_1^2 = r_2^2$$

which is not possible as $b - 1 = r^2 < c < 2s + cr_1^2 = r_2^2 \leq r^2$.

Assume now that (4.6) holds. Then

$$2s + r_1^2 = cr_2^2 \tag{4.7}$$

which is possible only when $r_2 = 1$, as $2s^2 \geq 2s + r^2 \geq 2s + r_1^2 = cr_2^2 > s^2r_2^2$. If $r_2 = 1$ then $r_1 = r$ and from (4.6) we have $t - s = r^2$. However this is not possible as $t \equiv s \pmod{r^2}$ implies by Definition 3.1 (equivalence of solutions) that $(t, s) \sim (b - r, 1 - r)$, which by Lemma 4.1 is not true.

The proofs in the cases when $c = 2p^k$ and $d = p$ are similar, where in the latter case we work as above with the equation $y^2 - x^2 = r^2d$.

8

Assume now that $s = p^k$. Considering (4.2) modulo 4 we see that t is odd and r is even. Therefore $\gcd(t + r, t - r) = 1$ or $\gcd(t + r, t - r) = p^m$ for some $m \geq 1$ (as $\gcd(t, r)|s$). From (4.2) we have $t^2 - r^2 = bs^2$ so that if $\gcd(t + r, t - r) = 1$, then for some factorization $b = b_1 b_2$ we have either

$$t - r = b_1 s^2, \ t + r = b_2 \tag{4.8}$$

or

$$t - r = b_1, \ t + r = b_2 s^2. \tag{4.9}$$

If (4.8) holds, then we have $b_1 s^2 + 2r = b_2 \leq b = 1 + r^2$ which is not possible as $r < s$. If (4.9) holds, then $2r + b_1 = b_2 s^2 \leq 2r + 1 + r^2$, which gives $b_2 = 1$, in which case from (4.9) we have $s = r + 1$ and $t = r^2 + s$. The latter is not possible as seen above in the proof of the case when $c = p$.

We assume now that $\gcd(t + r, t - r) > 1$ so that $t = p^m t_1$ and $r = p^m r_1$ where $\gcd(t_1, r_1) = 1$ and $1 \leq m \leq k$. Then (4.2) gives

$$t_1^2 - cr_1^2 = p^{2k-2m}, \tag{4.10}$$

which by Lemma 3.3 is not possible if $m < k$. If $m = k$, then $s|r$, which is not true as $r < s$.

Next we turn to the case when $s = 2p^k$. Note from (4.2) that either t and r are both even or both odd. Moreover

$$\left(\frac{t}{\gcd(t, r)}\right)^2 - c\left(\frac{r}{\gcd(t, r)}\right)^2 = \left(\frac{s}{\gcd(t, r)}\right)^2. \tag{4.11}$$

If $\gcd(t, r) = 2p^m$ with $0 \leq m < k$, the above equation by Lemma 3.3 is not possible. If $m = k$, we have $s|r$, which is again not possible. Having thus discarded the case when $\gcd(t, r)$ is even, we assume now that t and r are both odd. We first consider the case $\gcd(t, r) = 1$. It follows from (4.2) that $\gcd(t + r, t - r) = 2$ (note that $b \equiv 2 \pmod 4$). Moreover there is a factorization $b = b_1 b_2$ such that

$$t - r = 2b_1 p^{2k}, \ t + r = 2b_2 \tag{4.12}$$

or

$$t - r = 2b_2, \ t + r = 2b_1 p^{2k}. \tag{4.13}$$

Observe that if b_1 is even above, then (4.12) and (4.13) take the form of (4.8) and (4.9) and hence following the reasoning given therein we conclude that b_1 is odd.

9

Assume that (4.12) holds. Then we have $b_2 = r + b_1 p^{2k}$, which gives $1 + b_1 \frac{s^2}{4} = 1 + b_1 p^{2k} \leq r + b_1 p^{2k} \leq b = 1 + r^2$, so that $\frac{b_1}{4} \leq 1$. Therefore $b_1 = 1$ or 3, as b_1 is odd. We may discard the value 3 as $b = 1 + r^2$ is a sum of two co-prime squares. If $b_1 = 1$, then $b_2 = b$ and $b = r + p^{2k}$, which gives $p^{2k} = 1 + r^2 - r$. Hence $(r-1)^2 < p^{2k} < r^2$, that is, $r - 1 < p^k < r$, which is not possible. The case when (4.13) holds is analogous.

It remains to consider the case when $\gcd(t, r) > 1$, that is $t = p^m t_1$ and $r = p^m r_1$, where $m \geq 1$ and $\gcd(t_1, r_1) = 1$. We have from (4.2)

$$t_1^2 - c r_1^2 = 4 p^{2k-2m}, \tag{4.14}$$

that is the identity form $(1, 0, -c)$ primitively represents the integer $4p^{2k-2m}$. Note by Lemma 3.2 that $m < k$. It follows from Lemma 2.1 part 1, that $(1, 0, -c) \sim (4p^{2k-2m}, u, v)$ for some integers u, v. Using the composition formula (Definition 2.2) it is easy to verify that

$$(4p^{2k-2m}, u, v) \sim (4, u, vp^{2k-2m})(p^{2k-2m}, u, 4v)$$

and hence (as $(1, 0, -c) \sim (4p^{2k-2m}, u, v)$ represents the identity class)

$$(4, u, vp^{2k-2m}) \sim (p^{2k-2m}, -u, 4v). \tag{4.15}$$

From Lemma 2.1 part 3, there are only two classes of forms that represent 4, namely $(4, \pm 2, -p^{2k})$ and two classes of forms that represent p^{2k-2m}, namely, $(p^{2k-2m}, \pm 2, -4p^{2m})$. Therefore from (4.15) it follows that $(4, 2, -p^{2k})$ is equivalent either to the form $(p^{2k-2m}, 2, -4p^{2m})$, or to its inverse. In either case, as a form and its inverse represent the same integers, the form $(4, 2, -p^{2k})$ primitively represents both p^{2k-2m} and $-4p^{2m}$. As one of p^{2k-2m} or $4p^{2m}$ is less than or equal to s, we have by Lemma 3.2 that $2m = k$. Following the same reasoning used to obtain (4.12) and (4.13), we have, as $t_1^2 - r_1^2 = 4bp^k$, either

$$t_1 - r_1 = 2b_1 p^k, \ t_1 + r_1 = 2b_2 \tag{4.16}$$

or

$$t_1 - r_1 = 2b_2, \ t_1 + r_1 = 2b_1 p^k, \tag{4.17}$$

where $b = b_1 b_2$. If (4.16) holds then

$$b_2 = r_1 + p^k b_1$$

10

and hence $b = 1 + r^2 = 1 + p^k r_1^2 = b_1 b_2 = b_1 r_1 + p^k b_1^2$, so that

$$b_1 r_1 - 1 = p^k (r_1^2 - b_1^2) = p^k (r_1 + b_1)(r_1 - b_1).$$

It follows from the above equation that $b_1 < r_1$ and hence

$$p^k r_1 (r_1 - b_1) < p^k (r_1 + b_1)(r_1 - b_1) < r_1^2,$$

which implies that

$$\frac{s}{2} = p^k < \frac{r_1}{r_1 - b_1}.$$

As $r_1 = \frac{r}{p^{k/2}} < \frac{r}{2}$, the above equation yields $\frac{s}{2} < \frac{r}{2(r_1 - b_1)} \leq \frac{r}{2}$, a contradiction. We conclude the proof here for $s = 2p^k$ with some remarks in the case when (4.17) holds. Here we obtain $\frac{s}{2} < \frac{b_1}{b_1 - r_1}$. It may be shown that in this case $b_1 < b_2$ and hence $b_1 < r$, so that if $b_1 - r_1 \geq 2$, then we have the required contradiction of $s < r$. If $b_1 - r_1 = 1$, then $\frac{s}{2} < r_1 + 1 < \frac{r}{3} + 1$.

In the case of the integer x, note by Lemma 4.2 that x is divisible by the least common multiple of r and s. Therefore if x is not divisible by two distinct odd primes, then

$$r = 2^\alpha p^m, \quad s = 2^\beta p^n,$$

where m, n, α, β are non negative integers and p is an odd prime. Observe that $r|s$ is not possible as this implies by Definition 3.1 that the solutions $(r, 0)$ and (t, s) are equivalent, contradicting Lemma 4.1. It follows that $m = n$ is not possible, as in this case either $r|s$ (if $\alpha \leq \beta$), or $s|r$ (if $\beta \leq \alpha$). If $m < n$, then $\beta < \alpha$ (as $r \nmid s$) and $g = \gcd(t, s) = \gcd(t, r) = \gcd(r, s) = 2^\beta p^m$, so that from (4.2)

$$\left(\frac{t}{g}\right)^2 - c \left(\frac{r}{g}\right)^2 = p^{2n-2m},$$

which is not possible by Lemma 3.3. In the case when $n < m$, we conclude similarly, using (4.1).

Proof of Theorem 1.2

We have $n = \gcd(t, s)|r$. Note that $n \neq r$ as if $r|s$, then as seen in the proof above, by Definition 3.1 the solutions $(r, 0)$ and (t, s) are equivalent, which is not the case by Lemma 4.1. Therefore, if $n > 1$, then $n = p$ or $n = q$. If $t = nt_1$ and $s = ns_1$ with $\gcd(t_1, s_1) = 1$, then from (4.1) we have

$$t_1^2 - bs_1^2 = \left(\frac{r}{n}\right)^2 \tag{4.18}$$

11

which is not possible by Lemma 3.3. Thus $n = 1$ and we have two primitive solutions of $X^2 - bY^2 = r^2$, namely $(b - r, (r - 1))$ and (t, s). By Lemmas 4.1 and 4.3 it follows that p^4 and q^4 are primitively represented by the form $(1, 0, -b)$. Finally, Lemma 3.2 gives $p^4 > r$ and $q^4 > r$, which yields the desired result.

$\square$.

Proof of Corollary 1.3

If $b = (pq)^2 + 1$ and $pq \leq \alpha$, then by assumption the $D(-1)$ pair $\{1, b\}$ cannot be extended to a $D(-1)$ quadruple. Hence we assume that $pq > \alpha$. If $p \leq \alpha^{\frac{1}{4}} \leq (pq)^{\frac{1}{4}}$, then by Theorem 1.2 it follows that the $D(-1)$ pair $\{1, b\}$ cannot be extended to a $D(-1)$ quadruple.

$\square$

Proof of Theorem 1.5

If $\gcd(r, s) = 1$, then $\gcd(t, s) = 1$ and it follows from (4.1) and Lemma 4.1 that there are two primitive solutions of $X^2 - bY^2 = r^2$, namely $(b - r, (r - 1))$ and (t, s), that satisfy $(b - r, r - 1) \not\sim (t, \pm s)$. Therefore by Lemma 4.3, there exists a factorization $r = pq$, where p and q are coprime and both greater than 1, such that p^4 and q^4 are primitively represented by the form $(1, 0, -b)$. However as $r = P\phi$, at least one of p or q say p, divides $\phi < r^{\frac{1}{4}}$ and thus $p^4 < r$ which is not possible by Lemma 3.2.

$\square$

References

[1] D. Buell, *Binary quadratic forms*, 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), 318–338.

[4] A. Filipin and Y. Fujita , *The number of $D(-1)$-quadruples*, Math. Commun., **15** (2010), No. 2, 387–391.

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

[6] R. A. Mollin, *Quadratics*, CRC press, Boca Raton, 1996.

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