Proceedings of the Edinburgh Mathematical Society (2011) **54**, 25–32
DOI:10.1017/S0013091509000285 First published online 1 November 2010

ON THE GAPS BETWEEN VALUES OF BINARY QUADRATIC FORMS

JÖRG BRÜDERN* AND RAINER DIETMANN†

Institut für Algebra und Zahlentheorie, Universität Stuttgart, 70511 Stuttgart, Germany

(Received 2 March 2009)

Abstract Among the values of a binary quadratic form, there are many twins of fixed distance. This is shown in quantitative form. For quadratic forms of discriminant -4 or 8 a corresponding result is obtained for triplets.

Keywords: gaps; binary quadratic forms; Hasse principle

2010 *Mathematics subject classification:* Primary 11E16
Secondary 11E25

1. Introduction

The work of Goldston *et al.* [**6**] has revived interest in the study of the gaps in certain sequences, such as the primes, the sums of two squares or the values of norm forms (see, for example, [**5**, **7**, **10**]). Here we consider the values taken by binary quadratic forms and show that there are infinitely many proper twins of any prescribed distance unless this is prevented by a congruence obstruction. More precisely, let $q(x, y) = ax^2 + bxy + cy^2$ be a binary quadratic form with integer coefficients and discriminant $d = b^2 - 4ac$. Suppose that $d \neq 0$, and for $d < 0$ suppose further that q is positive definite. Let (s_n) denote the sequence of natural numbers representable by q, arranged in increasing order. A *proper twin* of distance k is a pair s_n, s_{n-1} with $s_n - s_{n-1} = k$. If such a twin exists, then the diophantine equation

$$q(x, y) - q(z, w) = k \tag{1.1}$$

is soluble. We show that the converse is true and, since (1.1) satisfies an integral Hasse principle, we obtain a local-to-global principle for gaps: *either* there are infinitely many proper twins of distance k *or* (1.1) has no solution in p-adic integers, for at least one prime p.

* Present address: Mathematisches Institut, Georg-August Universität Göttingen, Bunsenstrasse 3–5, 37073 Göttingen, Germany (bruedern@uni-math.gwdg.de).

† Present address: Department of Mathematics, Royal Holloway University of London, Egham TW20 0EX, UK (rainer.dietmann@rhul.ac.uk).

Theorem 1.1. *Let q be a binary quadratic form of discriminant $d \neq 0$, as above. Let k be a natural number and suppose that Equation (1.1) has a solution in p-adic integers for all primes $p|2d$. Then, for any $\varepsilon > 0$, one has*

$$\#\{s_n \leqslant X : s_n - s_{n-1} = k\} \gg X^{1-\varepsilon}.$$

The implicit constant may depend here on q, k and ε, of course. For comparison, we note that when d is not a square, there are, by an old result of Bernays [**1**], about $X(\log X)^{-1/2}$ values $s_n \leqslant X$, so, on average, the gap $s_n - s_{n-1}$ should be nearly as large as $(\log n)^{1/2}$.

As we shall see in § 2, Theorem 1.1 is a simple consequence of weak approximation for quaternary quadratic forms. We require the latter in quantitative form. A suitable version is contained in [**3**].

In some cases, the ideas underlying the proof of Theorem 1.1 can be coupled with an observation of Hooley [**8**] to establish the existence of proper triplets in the sequence (s_n). A *proper triplet* of distance k, l is a triple s_n, s_{n-1}, s_{n-2} with

$$s_n - s_{n-1} = k, \qquad s_{n-1} - s_{n-2} = l.$$

We discuss this only in two cases: for the intensely investigated sequence of sums of two squares and for the indefinite form $x^2 - 2y^2$. We conclude as follows.

Theorem 1.2. *Let (s_n) denote the sequence of natural numbers that are representable as the sum of two integral squares, arranged in increasing order. Then, for any pair $(k, l) \in \mathbb{N}^2$, there are infinitely many proper triplets of distance k, l in this sequence. The same is true if (s_n) is the sequence of values of the quadratic form $x^2 - 2y^2$.*

A proof of Theorem 1.2 is sketched out in §§ 3 and 4. Note that for the indefinite form $x^2 - 2y^2$, we enumerate the integral values, not only the positive ones. The method might also be able to be applicable to some other binary forms. However, a thorough treatment of triplets among the values of binary quadratic forms $q(x, y)$ will have to wait for the development of a more complete theory for the diophantine system

$$q(x, y) - q(z, w) = k, \qquad q(z, w) - q(u, v) = l. \tag{1.2}$$

For the forms covered by Theorem 1.2, solutions of (1.2) are found by a differencing argument and the theory of ternary quadratic forms. In the two cases covered by Theorem 1.2, only the ternary forms $X^2 + Y^2 - 2Z^2$ and $2X^2 + 2Y^2 - Z^2$ arise, and the class number is 1 for determinants -2 and 4. This is crucial for our method.

2. Twins

In this section, we prove Theorem 1.1. Fix a quadratic form q and $k \in \mathbb{N}$ as in that theorem. Let $\mathcal{P}(q)$ denote the set of all primes p for which the congruence $p|q(x, y)$ always implies $p|x$, $p|y$. Note that if n is an integer representable by q and $p \in \mathcal{P}(q)$ with $p|n$, then $p^2|n$. By the theory of binary quadratic forms, there are infinitely many primes

in $\mathcal{P}(q)$, and we now choose $k-1$ distinct such primes $p_1, \dots, p_{k-1}$, with $p_j > 2dk$ for all $1 \leqslant j \leqslant k-1$. Then $p_j \nmid 2d$ and $q(x,y)$ is therefore non-singular $\bmod p_j$. Since a non-singular binary form $\bmod p_j$ represents all non-zero residue classes $\bmod p_j$, there are integers ξ_j, η_j with $q(\xi_j, \eta_j) \equiv -j \bmod p_j$, and by Hensel's Lemma these can be chosen to satisfy $q(\xi_j, \eta_j) \equiv p_j - j \bmod p_j^2$. By the Chinese Remainder Theorem, we now find a pair $(\xi, \eta) \in \mathbb{Z}^2$ with

$$q(\xi, \eta) \equiv p_j - j \bmod p_j^2 \tag{2.1}$$

for all $1 \leqslant j \leqslant k-1$. Let $r = (p_1 p_2 \cdots p_{k-1})^2$. If $z \equiv \xi \bmod r$, $w \equiv \eta \bmod r$, then (2.1) implies that $q(z,w) + j \equiv p_j \bmod p_j^2$ holds for all $1 \leqslant j \leqslant k-1$. In particular, none of the integers $q(z,w)+1, q(z,w)+2, \dots, q(z,w)+k-1$ is representable by q. Consequently, any solution $x, y, z, w \in \mathbb{Z}$ of

$$q(x,y) - q(z,w) = k, \quad z \equiv \xi \bmod r, \ w \equiv \eta \bmod r, \tag{2.2}$$

corresponds to a twin $s_n = q(x,y)$, $s_{n-1} = q(z,w)$ of distance k, provided only that $q(z,w) > 0$.

It remains to show that (2.2) has many solutions in integers. As a prerequisite we construct solutions in p-adic integers for all primes p. First consider primes $p \nmid 2rd$. Then $q(x,y) - q(z,w)$ is a quaternary quadratic form with discriminant not divisible by p, and therefore represents all p-adic integers as x, y, z, w vary over p-adic integers. In particular, (1.1) has a solution in p-adic integers. This last conclusion remains true for $p|2d$, by assumption in Theorem 1.1. Recall that $(2d; r) = 1$, by choice of p_j, so that it remains to consider primes $p|r$. Then $p = p_j$ for some $1 \leqslant j \leqslant k-1$, and the p-adic analogue of (2.2) reads

$$q(x,y) - q(z,w) = k, \quad z \equiv \xi \bmod p^2, \ w \equiv \eta \bmod p^2. \tag{2.3}$$

Let $K = k + q(\xi, \eta)$. For $p = p_j > 2dk$, we have $K \equiv k - j \not\equiv 0 \bmod p_j$. Since $p = p_j \nmid 2d$, there is a solution $x', y' \in \mathbb{Z}$ of $q(x', y') \equiv K \bmod p$ that then lifts to a solution of $q(x,y) = K$ in p-adic integers; a solution of (2.3) in p-adic integers is now given by $x, y, z = \xi$, $w = \eta$.

We are ready to establish Theorem 1.1. By weak approximation for quaternary quadratic forms and the deliberations in the preceding paragraph, it follows that (2.2) has a solution in integers. By Theorem 2 of [**3**], we conclude that

$$\#\{x, y, z, w \in \mathbb{Z} : |x|, |y|, |z|, |w| \leqslant P, \ (2.2) \text{ holds}\} \gg P^2. \tag{2.4}$$

By Lemma 2 of [**9**], the estimate

$$\#\{z, w \in \mathbb{Z} : q(z,w) = m, \ |z| \leqslant P, \ |w| \leqslant P\} \ll P^{\varepsilon} \tag{2.5}$$

holds uniformly in $m \in \mathbb{N}$. If q is positive definite, then $q(z,w) > 0$ trivially holds unless $z = w = 0$, and the conclusion of Theorem 1.1 is immediate from (2.4), (2.5) and the discussion relating to (2.2) in the antepenultimate paragraph.

When q is indefinite, the above argument still applies but only yields twins of distance k among the *integers* represented by q. However, for indefinite q with $d \neq 0$, the equation

$q(u,v) = 0$ in $\mathbb{R}^2$ defines two distinct lines through the origin; these mark the sign changes of q. In particular, one always finds two real numbers $A < B$ such that within the sector $Au < v < Bu$, $v > 0$, one has $q(u,v) > 0$. We choose real numbers $C_1 < C_2, C_3 < C_4$ such that the box $C_1 \leqslant u \leqslant C_2$, $C_3 \leqslant v \leqslant C_4$ is part of this sector, and instead of the quantity considered in (2.4) we count solutions of (2.2) with

$$C_1P < x, z < C_2P, \qquad C_3P < y, w < C_4P. \tag{2.6}$$

Any solution of (2.2) satisfying these constraints has $q(z,w) > 0$, and the method underlying Theorem 2 of [**3**] still yields a lower bound $\gg P^2$ for the number of solutions of (2.2) with (2.6). We may now argue as before to obtain Theorem 1.1 for indefinite forms.

3. Triplets

We prove Theorem 1.2 in full detail for sums of two squares. For given values of $k, l \in \mathbb{N}$ write $h = k + l$. Certain fine details in our treatment of triplets of distance k, l among the sums of two squares depend on the distribution of k, l, h modulo 4, and we begin with the case where $h \equiv 2 \bmod 4$. A proper triplet of distance k, l yields a solution of the pair of equations

$$x^2 + y^2 - z^2 - w^2 = k, \qquad x^2 + y^2 - z_0^2 - w_0^2 = h. \tag{3.1}$$

This pair possesses an infinitude of integer solutions, as was shown by Hooley [**8**]. We shall define suitable congruence conditions, very similar to those in (2.2) and (2.3), that will be stipulated on z and w in (3.1) to ensure that the remaining solutions correspond to proper triplets. Hooley's method will then be used to solve (3.1) with the extra congruence conditions attached to z and w.

It will be convenient to write $H = \frac{1}{2}h + 1$. For any fixed value of j with $-l < j < k$, $j \neq 0$, there are infinitely many primes $p \equiv 3 \bmod 4$ with

$$\left(\frac{2(k-j) - H^2}{p}\right) = 1; \tag{3.2}$$

this follows by quadratic reciprocity and Dirichlet's theorem for primes in arithmetic progressions. For any j as above, we can therefore pick a prime $p_j \equiv 3, \bmod 4$ that satisfies (3.2) and $p_j \nmid j$, and that is as large as we like. By the argument leading to (2.1), one finds integers ξ, η such that

$$\xi^2 + \eta^2 \equiv p_j - j \bmod p_j^2 \tag{3.3}$$

holds simultaneously for $-l < j < k$, $j \neq 0$. Let

$$r = \prod_{\substack{-l<j<k \\ j\neq 0}} p_j^2. \tag{3.4}$$

We shall now show that the pair (3.1) has a solution in integers satisfying

$$z \equiv \xi \bmod r, \qquad w \equiv \eta \bmod r. \tag{3.5}$$

For this solution, (3.3) implies that z^2+w^2+j is divisible by p_j but not by p_j^2, and so is not a sum of two squares for $-l<j<k$, $j\neq 0$. By (3.1), $z^2+w^2+k, z^2+w^2, z^2+w^2-l$ is a proper triplet. By (3.5) and (3.3), we see that $z^2+w^2\equiv p_1-1 \bmod p_1^2$, whence $z^2+w^2>\frac{1}{2}p_1$. However, as remarked earlier, we can take p_1 as large as we like, and hence, on varying p_1, we obtain infinitely many triplets of distance k,l when $h\equiv 2 \bmod 4$.

To solve the simultaneous conditions (3.1) and (3.5), we consider solutions with $z_0=x-1$, $w_0=y+1$. The second equation in (3.1) then reduces to $2x-2y=h+2=2H$. Since H is even, we solve this linear equation by $x=v+\frac{1}{2}H$, $y=v-\frac{1}{2}H$, $v\in\mathbb{Z}$. Then $x^2+y^2=2v^2+\frac{1}{2}H^2$ and the first equation in (3.1) reduces to

$$2v^2-z^2-w^2=k-\tfrac{1}{2}H^2, \tag{3.6}$$

which we now need to solve with z,w in accordance with (3.5).

We discuss this problem in the p-adic integers $\mathbb{Z}_p$ first. The ternary quadratic form $X^2+Y^2-2Z^2$ is *universal*: that is, it represents all integers. Hence, for all primes p, (3.6) has a solution in $\mathbb{Z}_p$. For primes $p|r$ we have $p=p_j$ for some j and we wish to solve (3.6) in $\mathbb{Z}_p$, with $z\equiv\xi \bmod p^2$, $w\equiv\eta \bmod p^2$. We take $z=\xi$, $w=\eta$ to satisfy the congruence conditions. By (3.3) and (3.6), it remains to solve the congruence

$$2v^2\equiv k-\tfrac{1}{2}H^2+p_j-j \bmod p_j^2.$$

Since p_j is odd, we may multiply by 2 and then apply (3.2) to see that this congruence has a solution $\bmod p_j$, with $p_j\nmid v$. By Hensel's Lemma, this solution lifts to a solution $\bmod p_j^2$, and then to a solution in $\mathbb{Z}_p$.

This information is enough to solve the system (3.5) and (3.6). Up to equivalence, the form $X^2+Y^2-2Z^2$ is the only integral ternary quadratic form of determinant -2. Hence, by weak approximation for the *individual* form (and not only for its genus), there is an integral solution to (3.5) and (3.6). This completes the argument in the case where $h\equiv 2 \bmod 4$.

A simple variant applies when $h\equiv 0 \bmod 4$ but $k\not\equiv 2 \bmod 4$. The beginning is identical to the previous argument: we choose p_j, r, ξ, η exactly as before and we still intend to solve the equations in (3.1) with z, w subject to (3.5). Again, we solve the second equation in (3.1) by $z_0=x-1$, $w_0=y+1$ and $x-y=H$. Since H is now odd, we choose $2x=v+H$, $2y=v-H$, where v runs through odd integers. The first equation in (3.1) becomes

$$v^2-2z^2-2w^2=2k-H^2, \tag{3.7}$$

which we now have to solve simultaneously with (3.5). Note that $H\equiv 1 \bmod 2$ implies that v is necessarily odd, whence it suffices to solve (3.7) in integers.

We note that in the current context, H is odd and k is either also odd or divisible by 4. Hence, $2k-H^2$ is in one of the three residue classes $\pm 1 \bmod 8$, $5 \bmod 8$. In all these cases, (3.7) has a solution in integers [**2**, Theorem 56] and therefore in $\mathbb{Z}_p$. In the more important case $p|r$ we again have $p=p_j$, and we then need to solve (3.7) with $z\equiv\xi \bmod p^2$, $w\equiv\eta \bmod p^2$. We take $z=\xi$, $w=\eta$ and apply (3.3). We then solve

$$v^2\equiv 2(k+p_j-j)-H^2 \bmod p_j^2$$

by (3.2) and Hensel's Lemma; there is then also a solution in $\mathbb{Z}_p$ of (3.7) with $z \equiv \xi \bmod p^2$, $w \equiv \eta \bmod p^2$. The form $2X^2 + 2Y^2 - Z^2$ is the adjoint of $X^2 + Y^2 - 2Z^2$, in the sense of Gauss [**4**], and is therefore the only form of its determinant, up to equivalence. Thus, again by weak approximation, (3.7) and (3.5) have a simultaneous integer solution. This establishes Theorem 1.2 in the case $h \equiv 0 \bmod 4$, $k \not\equiv 2 \bmod 4$ as well.

Next, we discuss the case when $k \equiv 2 \bmod 4$, or when $k \equiv 0 \bmod 4$ but $h \not\equiv 2 \bmod 4$. In these cases, we can exchange the roles of h and k, and consequently of z, w and z_0, w_0, and proceed exactly as before, but we need to observe that a congruence condition will now be activated on z_0, w_0 and that $z_0^2 + w_0^2$ is the smallest member of the triplet to be found. Hence, rather than working with (3.2) in its original form, we put $K = \frac{1}{2}k + 1$ and then choose primes $p_j \equiv 3 \bmod 4$ with

$$\left(\frac{2(h-j) - K^2}{p_j}\right) = 1$$

for $1 \leqslant j \leqslant h-1$, $j \neq l$. With r now the product of all these p_j^2 as a substitute for (3.4), one chooses $\xi, \eta \in \mathbb{Z}$ in accordance with (3.3), for the new range of j. We then need to solve (3.1) with $z_0 \equiv \xi \bmod r$, $w_0 \equiv \eta \bmod r$, and this can be done *mutatis mutandis*.

The only remaining case is when h and k are both odd. Then $l = h - k$ is even and, in place of (3.1), we study the pair of equations

$$z^2 + w^2 - x^2 - y^2 = h, \qquad z_0^2 + w_0^2 - x^2 - y^2 = l \tag{3.8}$$

with a congruence condition attached to z and w that ensures that $z^2 + w^2 - j$ is not a sum of two squares for $1 \leqslant j \leqslant h-1$, $j \neq k$. For $l \equiv 2 \bmod 4$, this again leads to the arithmetic of $X^2 + Y^2 - 2Z^2$, as in the case $h \equiv 2 \bmod 4$, and for $l \equiv 0 \bmod 4, h$ odd, we are led to the adjoint form, again as in the treatment for $h \equiv 0(4)$, $k \not\equiv 2(4)$. Details are left to the reader.

4. Triplets, yet again

The treatment of the sums of two squares now being complete, we turn to the values of the indefinite form $x^2 - 2y^2$. The chase for triplets of distance k, l this time depends on the distribution of the exact powers of 2 that divide the numbers k, l and $h = k + l$. Write $k = 2^\kappa k'$, $l = 2^\lambda l'$ and $h = 2^\mu h'$ with odd natural numbers k', l', h'. Two of the three numbers κ, λ, μ must then be equal and the remaining one is necessarily larger than the equal ones.

A simple observation reduces the number of cases that we need to consider. The forms $x^2 - 2y^2$ and $2x^2 - y^2$ are equivalent; hence a number $n \in \mathbb{Z}$ is represented by $x^2 - 2y^2$ if and only if $-n$ is represented. Consequently, if $s_n - s_{n-1} = k$, $s_n - s_{n-2} = h$ is a triplet of distance k, l, then $-s_{n-2}, -s_{n-1}, -s_n$ is a triplet of distance l, k. Therefore, it suffices to establish the existence of triplets only in the case where $\kappa \leqslant \lambda$.

We first discuss the case where $\kappa < \lambda$. In this case, as we have just observed, $\kappa = \mu$. Our strategy is to solve the pair of equations

$$x^2 - 2y^2 - z^2 + 2w^2 = k', \qquad x^2 - 2y^2 - z_0^2 + 2w_0^2 = h' \tag{4.1}$$

with an additional congruence condition that we now define. For any $j \in \mathbb{Z}$ with $-l < j < k$, $j \neq 0$, there are infinitely many primes p with $p \equiv 3 \bmod 8$ and

$$\left(\frac{k' + H^2 - \bar{2}^\kappa j}{p}\right) = -1, \tag{4.2}$$

where $H = \frac{1}{2}(h' - 1)$ and $\bar{2}$ is defined by $\bar{2}2 \equiv 1 \bmod p_j$. Again, this is easily seen by quadratic reciprocity and Dirichlet's theorem on primes in arithmetic progressions and we pick one such prime: p_j, say. These are all odd, and the form $\xi^2 - 2\eta^2$ is non-singular $\bmod p_j$. We may therefore solve the congruence

$$2^\kappa(\xi^2 - 2\eta^2) \equiv p_j - j \bmod p_j^2 \tag{4.3}$$

in integers $\xi, \eta \in \mathbb{Z}$ simultaneously for all $-l < j < k$, $j \neq 0$. Define r by (3.4) and let us suppose that a solution of (4.1) can be found that also satisfies (3.5). The numbers $s = x^2 - 2y^2$, $s' = z^2 - 2w^2$ and $s'' = z_0 - 2w_0^2$ are all then values of the binary form $X^2 - 2Y^2$. By the elementary theory of $\mathbb{Q}(\sqrt{2})$, the numbers $S = 2^\kappa s$, $S' = 2^\kappa s'$ and $S'' = 2^\kappa s''$ are again values of this form. By (4.1), we have $S - S' = k$, $S - S'' = h$ and, by (4.3), we have $S' \equiv p_j - j \bmod p_j^2$. In particular, $S' + j$ is not a value of $X^2 - 2Y^2$ for $-l < j < k$, $j \neq 0$. Hence, S, S', S'' is a triplet of distance k, l. Moreover, $|S'| \geqslant p_1 - 1$ by (4.3), and by varying p_1 we obtain infinitely many such triplets.

Thus, we are reduced to solving (4.1) with (3.5). Take $z_0 = x + 1$, $w_0 = y + 1$. The second equation in (4.1) then reduces to $4y - 2x = h' - 1$. Write $H = \frac{1}{2}(h' - 1)$ and solve by $x = 2v + H$, $y = v + H$. Then $x^2 - 2y^2 = 2v^2 - H^2$ so that the simultaneous conditions (4.1), (3.5) reduce to

$$2v^2 + 2w^2 - z^2 = k' + H^2, \quad z \equiv \xi \bmod r,\ w \equiv \eta \bmod r. \tag{4.4}$$

As remarked earlier, the form $2v^2 + 2w^2 - z^2$ represents all odd integers not congruent to $5 \bmod 8$. It also represents all even integers, because $2v^2 + 2w^2 - z^2 = 2t$ implies $z = 2z'$, and the equation $v^2 + w^2 - 2z'^2 = t$ is soluble in integers, by the universality of this form. In particular, we see that whenever $k' + H^2 \not\equiv 5 \bmod 8$, the equation in (4.4) has an integer solution. Now, for $p|r$, we have $p = p_j$ for some j. By (4.3),

$$k' + H^2 + \xi^2 - 2\eta^2 \equiv k' + H^2 - \bar{2}^\kappa j \bmod p_j,$$

and the right-hand side is a quadratic non-residue by (4.2). Since $(2/p_j) = -1$, it follows that $2v^2 \equiv k' + H^2 + \xi^2 - 2\eta^2 \bmod p_j$ has a solution with $p_j \nmid v$. By Hensel's Lemma, it follows that the equation in (4.4) has a solution in $\mathbb{Z}_{p_j}$, with $z \equiv \xi \bmod p_j^2$, $w \equiv \eta \bmod p_j^2$. As in our discussion of sums of two squares, weak approximation now yields an integer solution of (4.4). This completes the argument unless we are in the situation where $k' + H^2 \equiv 5 \bmod 8$, and this happens if and only if $h' \equiv 1 \bmod 8$ and $k' \equiv 5 \bmod 8$ or vice versa. In this exceptional case, we write $l = 2^\kappa l''$ so that $l'' = h' - k'$ and we study the system

$$x^2 - 2y^2 - z^2 + 2w^2 = l'', \qquad x^2 - 2y^2 - z_0^2 + 2w_0^2 = h'. \tag{4.5}$$

As in the case of sums of two squares, the congruence conditions (3.5) now have to be activated through suitable analogues of (4.2), with a different range for j. As this should now be familiar, we spare the reader the details. The differencing process $z_0 = x + 1$, $w_0 = y + 1$ leads to the equation $2v^2 + 2w^2 - z^2 = l'' + H^2$ as the analogue of (4.4). Here $l'' + H^2$ is even, so this equation has integer solutions. The rest of the argument can be performed as before and one finds that the appropriate version of (3.5) can be accommodated. This completes the discussion of the case $\kappa < \lambda$. If $\kappa = \lambda$, then we begin with (4.5) where $l'' = l'$ is now odd. One may proceed as before unless one is in the exceptional situation where $l' \equiv 1 \bmod 8$, $h' \equiv 5 \bmod 8$ or vice versa. In the latter case, we have to use a pair of the type (4.1) with k' replaced by $h' - l'$. We leave it to the reader to work out the relevant congruence conditions to complete the proof of this part of Theorem 1.2.

References

1. P. Bernays, Über die Darstellung von positiven, ganzen Zahlen durch die primitiven binären quadratischen Formen einer nichtquadratischen Diskriminante, Dissertation, Universität Göttingen (1912).
2. L. E. Dickson, *Studies in the theory of numbers* (Chicago University Press, 1930).
3. R. Dietmann, Small solutions of quadratic Diophantine equations, *Proc. Lond. Math. Soc.* **86** (2003), 545–582.
4. C. F. Gauss, *Disquisitiones arithmeticae* (Leipzig, 1801).
5. D. A. Goldston, S. W. Graham, J. Pintz and C. Y. Yildirim, Small gaps between products of two primes, *Proc. Lond. Math. Soc. (3)* **98** (2009), 741–774.
6. D. A. Goldston, J. Pintz and C. Y. Yildirim, Primes in tuples, I, *Annals Math. (2)* **170** (2009), 819–862.
7. M. Hablizel, Beschränkte Lücken zwischen Werten von Normformen, Dissertation, Universität Stuttgart (2008).
8. C. Hooley, On the intervals between numbers that are sums of two squares, II, *J. Number Theory* **5** (1973), 215–217.
9. P. Lefton, On the Galois groups of cubics and trinomials, *Acta Arith.* **35** (1979), 239–246.
10. F. Thorne, Bounded gaps between products of primes with applications to ideal class groups and elliptic curves, *Int. Math. Res. Not.* **2008**(5) (2008), rnm156.