Mathematika 62 (2016) 551–571 © 2016 University College London
doi:10.1112/S0025579315000364

SMALL SOLUTIONS OF QUADRATIC CONGRUENCES, AND CHARACTER SUMS WITH BINARY QUADRATIC FORMS

D. R. HEATH-BROWN

Abstract. Let $Q(x, y, z)$ be an integral quadratic form with determinant coprime to some modulus q. We show that $q \mid Q$ for some non-zero integer vector (x, y, z) of length $O(q^{5/8+\varepsilon})$, for any fixed $\varepsilon > 0$. Without the coprimality condition on the determinant one could not necessarily achieve an exponent below $2/3$. The proof uses a bound for short character sums involving binary quadratic forms, which extends a result of Chang.

§1. *Introduction.* Let $Q(\mathbf{x}) = Q(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ be a quadratic form. This paper, which may be seen as a continuation of the author's earlier work [**10**, **11**] seeks to understand the smallest solution of the congruence $Q(\mathbf{x}) \equiv 0 \pmod q$ in non-zero integers $\mathbf{x}$. Thus we shall set

$$m(Q; q) := \min\{\|\mathbf{x}\| : \mathbf{x} \in \mathbb{Z}^n - \{\mathbf{0}\}, Q(\mathbf{x}) \equiv 0 \pmod q\},$$

where $\|\mathbf{x}\|$ denotes the Euclidean norm, and ask (in the first instance) about

$$B_n(q) := \max_Q m(Q; q),$$

where the maximum is taken over all integral quadratic forms in n variables. (This definition differs slightly from that used in [**10**, **11**].) The interested reader may refer to Baker [**1**, Ch. 9] for an account of this problem and its applications.

It is trivial that $B_n(q)$ is non-increasing as a function of n. When q is square-free, it is easy to see that $B_n(q) = q$ for $n = 1$ or 2. Moreover, the form $Q(\mathbf{x}) = x_1^2 + \cdots + x_n^2$ has $m(Q; q) \geqslant q^{1/2}$ so that $B_n(q) \geqslant q^{1/2}$ for every q and every n. When $n = 3$ and q is square-free,

$$B_3(q) \geqslant m(Q; q) \geqslant q^{2/3} + O(q^{1/3})$$

for a suitable singular form

$$Q(x_1, x_2, x_3) = (x_1 - bx_2)^2 - a(x_2 - bx_3)^2. \tag{1.1}$$

(Details for the case in which q is prime are given in [**10**, Theorem 3] but the argument readily extends to any square-free q.) It is reasonable to conjecture that such lower bounds represent the true order of magnitude for $B_n(q)$ in general, so that

$$B_n(q) \ll_\varepsilon \begin{cases} q^{2/3+\varepsilon}, & n = 3, \\ q^{1/2+\varepsilon}, & n \geqslant 4, \end{cases}$$

for any fixed $\varepsilon > 0$ (uniformly in n, by the non-increasing property).

Received 18 November 2014, published online 18 February 2016.
MSC (2010): 11D79 (primary), 11L40, 11E20 (secondary).

https://doi.org/10.1112/S0025579315000364 Published online by Cambridge University Press

A basic upper bound for $B_n(q)$ was provided by Schinzel *et al* [16], who showed that

$$B_n(q) \ll \begin{cases} q^{1/2+1/(2n)}, & n \text{ odd}, \\ q^{1/2+1/(2n-2)}, & n \text{ even}. \end{cases}$$

In particular, one sees that $q^{2/3}$ is the true order of magnitude of $B_3(q)$, at least when q is square-free.

For $n \geqslant 4$ and any $\varepsilon > 0$ one has

$$B_n(q) \ll_\varepsilon q^{1/2+\varepsilon}$$

if q has at most two prime factors (see the author [11, Theorem 1]); that

$$B_4(q) \ll_\varepsilon q^{5/8+\varepsilon}$$

(see [11, Theorem 2]); and

$$B_n(q) \ll_{\varepsilon,n} q^{1/2+3/n^2+\varepsilon}$$

for every even $n \geqslant 12$ (see [11, Theorem 3]). Indeed, a number of other such bounds are possible.

It might appear from the above discussion that our question is completely resolved for $n = 3$, but wide open for $n \geqslant 4$. None the less, the main goal of this paper is a further exploration of the situation for $n = 3$ (!) It will be observed that the example (1.1) is a singular form. It turns out that one can do better by restricting attention to ternary forms which are non-singular modulo q. Before stating our result, we should make two simple observations. Firstly, if $q = q_0^2 q_1$ and $q_1 \mid Q(\mathbf{x})$, then $q \mid Q(q_0\mathbf{x})$. It follows that $m(Q; q) \leqslant q_0 m(Q; q_1)$. In particular, if we have proved that $B_n(q) \ll q^\theta$ for all square-free q and for some exponent $\theta \geqslant \frac{1}{2}$, then we may deduce that $B_n(q) \ll q^\theta$ for every q. Secondly, if $q = 2q_1$ and $q_1 \mid Q(\mathbf{x})$, then $q \mid Q(2\mathbf{x})$. It follows, in this case, that $m(Q; q) \leqslant 2m(Q; q_1)$. Once again, if we have proved that $B_n(q) \ll q^\theta$ for all odd square-free q and for some exponent θ, then we may deduce that $B_n(q) \ll q^\theta$ for every square-free q. These observations allow us to focus on odd square-free q. Indeed, we shall assume, without further comment, throughout the remainder of this paper that q is odd and square-free. In this situation, we can represent $Q(\mathbf{x})$ modulo q via a symmetric integer matrix, which we also denote by Q, by abuse of notation.

We now define

$$B_3^*(q) := \max_Q m(Q; q),$$

where the maximum is taken over all integral ternary quadratic forms Q with $(\det(Q), q) = 1$. This notation allows us to state our principal result.

THEOREM 1. *Let $q \in \mathbb{N}$ be odd and square-free, and let $\varepsilon > 0$ be given. Then*

$$B_3^*(q) \ll_\varepsilon q^{5/8+\varepsilon}.$$

https://doi.org/10.1112/S0025579315000364 Published online by Cambridge University Press

So we see that we can go below the exponent $2/3$ which is the limiting exponent for $B_3(q)$. We now have the same exponent $5/8$ for (non-singular) forms in three variables as we previously had for four variables. (However, it is explained in [**11**] that one can reduce the exponent to $13/21$ with more work, in the four variable case.)

It now seems that one should conjecture a bound

$$B_3^*(q) \ll_\varepsilon q^{1/2+\varepsilon}. \tag{1.2}$$

The proof of Theorem 1 proceeds by reducing the problem to a second question, which we now explain. If Q is a quadratic form in $n \geqslant 2$ variables, we write

$$\widehat{m}(Q; q) := \min\{\|\mathbf{x}\| : \mathbf{x} \in \mathbb{Z}^n - \{\mathbf{0}\}, \exists t \in \mathbb{Z},\ Q(\mathbf{x}) \equiv t^2 \pmod q\}$$

and

$$\widehat{B}_n(q) := \max_Q \widehat{m}(Q; q),$$

where the maximum is taken over all integral quadratic forms in n variables such that $(\det(Q), q) = 1$.

We then have the following result.

LEMMA 1. *Let $q \in \mathbb{N}$ be odd and square-free. Then if Q is a ternary quadratic form with $(\det(Q), q) = 1$,*

$$m(Q; q) \ll q^{1/2} \widehat{m}(-Q^{\mathrm{adj}}; q)^{1/2},$$

where Q^{adj} is the adjoint matrix for Q. In particular,

$$B_3^*(q) \ll q^{1/2} \widehat{B}_3(q)^{1/2}.$$

This naturally leads us to speculate about the size of $\widehat{B}_3(q)$, and the natural conjecture is that

$$\widehat{B}_3(q) \ll_\varepsilon q^\varepsilon \tag{1.3}$$

for any fixed $\varepsilon > 0$. Of course, Lemma 1 immediately shows that this latter conjecture implies (1.2).

In view of Lemma 1, it is natural to change our focus from the form Q to $-Q^{\mathrm{adj}}$, and indeed we will switch notation so that it is now $\widehat{m}(Q; q)$, which will be our primary concern. If q is odd and square-free there is a real character

$$\chi_d(m) = \left(\frac{m}{d}\right)$$

for each divisor d of q, and the congruence $Q(\mathbf{x}) \equiv t^2 \pmod q$ will have a solution t if and only if

$$\sum_{d|q} \chi_d(Q(\mathbf{x})) > 0.$$

https://doi.org/10.1112/S0025579315000364 Published online by Cambridge University Press

We can therefore attempt to show that $\widehat{B}_3(q)$ is small by investigating the character sums

$$S(\chi, B, Q) := \sum_{\|\mathbf{x}\| \leqslant B} \chi(Q(\mathbf{x}))$$

for primitive characters χ to modulus $d > 1$. If we can show that

$$S(\chi, B, Q) \ll B^{3-\delta} \tag{1.4}$$

for some fixed $\delta > 0$, for every primitive χ to modulus $d \geqslant 2$, then we will be able to deduce that $\widehat{m}_3(Q; q) \leqslant B$, since one has $S(1, B, Q) \gg B^3$ for the trivial character.

It seems plausible that (1.4) should hold for $B \geqslant q^\eta$, for any fixed $\eta > 0$ and with $\delta = \delta(\eta) > 0$. This would suffice for (1.3), and hence also for (1.2).

One standard procedure to estimate sums such as $S(\chi, B, Q)$ is to complete the sum and use bounds of Weil–Deligne type. It is very instructive to carry this out in detail. If $d = q$ is prime, for example, and χ is the quadratic character, one finds on completing the exponential sum that

$$S(\chi, B, Q) = \frac{B^3}{q^3} \sum_{\mathbf{y} \pmod q} W\left(\frac{q}{B}\mathbf{y}\right) S(\mathbf{y}),$$

where $W \ll 1$ is a suitable weight function and

$$\begin{aligned} S(\mathbf{y}) &:= \sum_{\mathbf{x} \pmod q} e_q(\mathbf{y} \cdot \mathbf{x}) \left(\frac{Q(\mathbf{x})}{q}\right) \\ &= \tau_q^{-1} \sum_{m \pmod q} \left(\frac{m}{q}\right) \sum_{\mathbf{x} \pmod q} e_q(\mathbf{y} \cdot \mathbf{x} + m Q(\mathbf{x})). \end{aligned}$$

These complete sums can be computed explicitly. Assuming that $q \nmid \det(Q)$, the inner sum above is

$$\tau_q^3 \left(\frac{m \det(Q)}{q}\right) e_q(-\overline{4m} Q^{-1}(\mathbf{y})).$$

One then finds that $S(\mathbf{y})$ is of order q^2 when $q \mid Q^{\mathrm{adj}}(\mathbf{y})$, and of order q otherwise. This may be something of a surprise, since one typically expects complete sums in n variables to have size around $q^{n/2}$, and here $n = 3$. As a result, this analysis leads to a bound which one may think of as

$$S(\chi, B, Q) \ll_\varepsilon q^\varepsilon (q + B^3 q^{-1} \#\{\mathbf{y} \ll q/B : q \mid Q^{\mathrm{adj}}(\mathbf{y})\}).$$

Recall that we have estimated $m(R; q)$, say, for a ternary form R, in terms of sums $S(\chi, B, -R^{\mathrm{adj}})$. Thus it is apparent that the above analysis ultimately connects small solutions of $q \mid R(\mathbf{x})$ with small solutions of $q \mid R(\mathbf{y})$. In fact, the argument is not completely circular (because the relevant bounds $q^{1/2}B^{1/2}$ and q/B are different), and one can show in this way that $B_3^*(q) \ll_\varepsilon q^{2/3+\varepsilon}$, at least

https://doi.org/10.1112/S0025579315000364 Published online by Cambridge University Press

when q is prime. Alternatively, one can provide an upper bound for

$$\#\{\mathbf{y} \ll q/B : q \mid Q^{\mathrm{adj}}(\mathbf{y}), \mathbf{y} \text{ primitive}\}$$

from first principles, by using $O((q/B)^{3/2})$ plane slices of the type $\mathbf{a} \cdot \mathbf{y} = 0$. Each such slice produces a binary quadratic form of rank one or two, which will have $O(1)$ primitive zeros modulo q, under the assumption that q is prime. In this way one finds that

$$\#\{\mathbf{y} \ll q/B : q \mid Q^{\mathrm{adj}}(\mathbf{y})\} \ll (q/B)^{3/2},$$

and hence

$$S(\chi, B, Q) \ll_\varepsilon q^\varepsilon (q + B^{3/2} q^{1/2}).$$

We therefore have a non-trivial bound for $B \geqslant q^{1/3+\delta}$. Unfortunately, this merely yields $\widehat{B}_3(q) \ll_\varepsilon q^{1/3+\varepsilon}$ and hence $B_3^*(q) \ll q^{2/3+\varepsilon}$.

We have been unable to obtain a non-trivial bound for $S(\chi, B, Q)$ when $B \leqslant q^{1/3}$. However, if one replaces Q by a binary form one can do better. Indeed the following result of Chang [7, Theorem 11] is the main inspiration for this paper.

THEOREM 2 (Chang). *For any $\varepsilon > 0$ there is a corresponding $\delta > 0$ such that*

$$\left| \sum_{X' < x \leqslant X + X'} \sum_{Y' < y \leqslant Y + Y'} \chi(x^2 + axy + by^2) \right| < p^{-\delta} XY$$

for any non-trivial character χ modulo p, any $X, Y > p^{1/4+\varepsilon}$ and any integers a, b with $a^2 \not\equiv 4b \pmod p$.

This improves on the corresponding results of Burgess [5] and [6], which were non-trivial only for $X, Y > p^{1/3+\varepsilon}$.

The proof of Chang's result crucially uses the fact that a binary quadratic form over $\mathbb{F}_p$ factors over $\mathbb{F}_{p^2}$, and of course this limits the approach to the case $n = 2$. Since we are interested in composite q, we will require a variant of Theorem 2. The argument in [7] splits into two rather different cases, one in which the form factors over $\mathbb{F}_p$, and one in which it does not. In order to handle composite q we need to devise a treatment which handles both cases in the same way. Our result is the following.

THEOREM 3. *Let $\varepsilon > 0$ and an integer $r \geqslant 3$ be given, and suppose that $C \subset \mathbb{R}^2$ is a convex set contained in a disc $\{\mathbf{x} \in \mathbb{R}^2 : \|\mathbf{x} - \mathbf{x}_0\| \leqslant R\}$. Let $q \geqslant 2$ be odd and square-free, and let χ be a primitive character to modulus q. Then if $Q(x, y)$ is a binary quadratic form with $(\det(Q), q) = 1$,*

$$\sum_{(x,y) \in C} \chi(Q(x, y)) \ll_{\varepsilon, r} R^{2-1/r} q^{(r+2)/(4r^2)+\varepsilon}$$

for $q^{1/4+1/2r} \leqslant R \leqslant q^{5/12+1/2r}$.

https://doi.org/10.1112/S0025579315000364 Published online by Cambridge University Press

For comparison, we observe that the standard Burgess bound [4, Theorem 2] yields

$$\sum_{x,y\leqslant R}\chi(xy)\ll_{\varepsilon,r} R^{2-2/r}q^{(r+1)/(2r^2)+\varepsilon},$$

relative to which our theorem has a loss of $(Rq^{-1/4})^{1/r}$. In §3 we will apply Theorem 3 with $C=\{\mathbf{x}\in\mathbb{R}^2:\|\mathbf{x}\|\leqslant R\}$ and $R=q^{1/4+\delta}$. Taking $r>(2\delta)^{-1}$ we will be able to deduce that $\widehat{B}_2(q)\ll_\varepsilon q^{1/4+\delta}$. We then go on to conclude that $\widehat{B}_3(q)\ll_\varepsilon q^{1/4+\varepsilon}$ and hence, via Lemma 1, that $B_3^*(q)\ll q^{5/8+\varepsilon}$.

Before embarking on the proofs, we need to mention one point of notation. We shall follow the common convention that the small positive number ε will be allowed to change between appearances, allowing us to write $q^\varepsilon\log q\ll_\varepsilon q^\varepsilon$, for example.

§2. *Proof of Lemma 1.* Suppose that $-Q^{\mathrm{adj}}(\mathbf{a})\equiv t^2\pmod q$ with $\|\mathbf{a}\|=\widehat{m}(-Q^{\mathrm{adj}};q)$ and $\mathbf{a}\neq\mathbf{0}$. Write $\mathbf{a}=\alpha\mathbf{a}_0$ with $\alpha\in\mathbb{N}$ and $\mathbf{a}_0$ primitive, and let

$$\Lambda:=\{\mathbf{x}\in\mathbb{Z}^3:\mathbf{a}_0\cdot\mathbf{x}=0\}.$$

This will be a two-dimensional lattice of determinant $\|\mathbf{a}_0\|$. Let $\mathbf{x}_1$ be the shortest non-zero vector in Λ, and $\mathbf{x}_2$ the shortest vector non-proportional to $\mathbf{x}_1$. Then $\mathbf{x}_1$ and $\mathbf{x}_2$ form a basis for Λ, and

$$\|\mathbf{x}_1\|\cdot\|\mathbf{x}_2\|\ll\|\mathbf{a}_0\| \tag{2.1}$$

and

$$\mathbf{x}_1\wedge\mathbf{x}_2=\pm\mathbf{a}_0.$$

Here

$$(u_1,u_2,u_3)\wedge(v_1,v_2,v_3)=(u_2v_3-u_3v_2,u_3v_1-u_1v_3,u_1v_2-u_2v_1)$$

is the usual vector product. We proceed to write $R(u,v):=Q(u\mathbf{x}_1+v\mathbf{x}_2)$, so that R is a binary quadratic form. This gives

$$\det(R)=\det(Q(u\mathbf{x}_1+v\mathbf{x}_2))=Q^{\mathrm{adj}}(\mathbf{x}_1\wedge\mathbf{x}_2)=Q^{\mathrm{adj}}(\mathbf{a}_0)$$

as an identity, so that

$$-\alpha^2\det(R)=-Q^{\mathrm{adj}}(\mathbf{a})\equiv t^2\pmod q.$$

Let $(q,\alpha)=q_0$ and $q=q_0q_1$. If p is an odd prime factor of q_1, the form R will factor over $\mathbb{F}_p$ if its discriminant is a square modulo p. Since q is odd and square-free, it follows that q_1 is also odd and square-free. Moreover, the discriminant of R is $-4\det(R)$. Thus R factors over $\mathbb{F}_p$ for every prime factor p of q_1, and we may then use the Chinese remainder theorem to produce integral linear forms L_1 and L_2 such that $R(u,v)\equiv L_1(u,v)L_2(u,v)\pmod{q_1}$.

https://doi.org/10.1112/S0025579315000364 Published online by Cambridge University Press

Our next move is to find a short non-zero integer vector (u, v) such that $q_1 \mid L_1(u, v)$. Once we have done this we will automatically have $q_1 \mid R(u, v)$. Referring to the definition of the form R, we then see that $q_1 \mid Q(u\mathbf{x}_1 + v\mathbf{x}_2)$. Thus, if we take $\mathbf{x} = q_0(u\mathbf{x}_1 + v\mathbf{x}_2)$, we will have $q \mid Q(\mathbf{x})$, as required. Our task is therefore to show that there is a suitable vector (u, v) for which the corresponding $\mathbf{x}$ is sufficiently small.

Let

$$U := \left(q_1 \frac{\|\mathbf{x}_2\|}{\|\mathbf{x}_1\|}\right)^{1/2} \quad \text{and} \quad V := \left(q_1 \frac{\|\mathbf{x}_1\|}{\|\mathbf{x}_2\|}\right)^{1/2},$$

so that $UV = q_1$. Then an easy application of the pigeon-hole principle shows that one can find $(u, v) \in \mathbb{Z}^2 - \{(0, 0)\}$ with $q_1 \mid L_1(u, v)$ and satisfying $|u| \leqslant U$ and $|v| \leqslant V$. We then deduce that

$$\begin{aligned}
\|\mathbf{x}\| &= q_0\|u\mathbf{x}_1 + v\mathbf{x}_2\| \\
&\leqslant q_0(U\|\mathbf{x}_1\| + V\|\mathbf{x}_2\|) \\
&= 2q_0(q_1\|\mathbf{x}_1\| \cdot \|\mathbf{x}_2\|)^{1/2} \\
&\ll q_0(q_1\|\mathbf{a}_0\|)^{1/2} \\
&= q^{1/2}(q_0\|\mathbf{a}_0\|)^{1/2} \\
&\leqslant q^{1/2}(\alpha\|\mathbf{a}_0\|)^{1/2} \\
&= q^{1/2}\|\mathbf{a}\|^{1/2}
\end{aligned}$$

by (2.1). Since $\mathbf{x}$ must be non-zero we deduce that

$$m(Q; q) \ll (q\|\mathbf{a}\|)^{1/2} = q^{1/2}\widehat{m}(-Q^{\text{adj}}; q)^{1/2},$$

as required.

§3. *Deduction of Theorem 1.* In this section, we will show how Theorem 1 follows from Theorem 3. Clearly, it suffices to prove that $\widehat{m}(Q; q) \ll_\varepsilon q^{1/4+\varepsilon}$ uniformly for any ternary form Q with $(\det(Q), q) = 1$.

Our first task is to establish the following corollary to Theorem 3.

LEMMA 2. *For any $\delta > 0$ there is a corresponding $\eta > 0$ such that, if $q > 1$ and $C \subset \mathbb{R}^2$ is a convex set contained in a disc $\{\mathbf{x} \in \mathbb{R}^2 : \|\mathbf{x} - \mathbf{x}_0\| \leqslant R\}$,*

$$\sum_{(x,y)\in C} \chi(Q(x, y)) \ll_\delta R^{2-\eta}$$

for $R \geqslant q^{1/4+\delta}$, uniformly for every primitive character χ modulo q and for every binary quadratic form Q with $(\det(Q), q) = 1$.

We prove this in three steps, beginning with the case in which $q^{1/4+\delta} \leqslant R \leqslant q^{5/12}$. In this range we choose

$$r = 3 + [1/\delta], \qquad \eta = 1/(r^2 + 4r) \quad \text{and} \quad \varepsilon = \eta/4.$$

https://doi.org/10.1112/S0025579315000364 Published online by Cambridge University Press

Then $r \geqslant 3$ and $1/4 + \delta \geqslant 1/4 + 1/r$, so that

$$q \leqslant R^{1/(1/4+\delta)} \leqslant R^{4r/(r+4)}.$$

Thus Theorem 3 produces

$$\begin{aligned}\sum_{(x,y)\in C} \chi(Q(x,y)) &\ll_{\varepsilon,r} R^{2-1/r} q^{(r+2)/(4r^2)+\varepsilon} \\ &\ll_{\delta} R^{2-1/r+(r+2)/r(r+4)+4\varepsilon} \\ &= R^{2-2/r(r+4)+\eta} \\ &= R^{2-\eta}.\end{aligned}$$

Next, when $q^{5/12} \leqslant R \ll q$, we cover $\mathbb{R}^2$ with disjoint squares of side $q^{5/12}$ to obtain a partition of C into $O(R^2 q^{-5/6})$ convex subsets, each with diameter at most $q^{5/12}$. On applying the result above with $\delta = 1/6$ we find that

$$\sum_{(x,y)\in C} \chi(Q(x,y)) \ll R^2 q^{-5/6} (q^{5/12})^{2-\eta} \ll R^{2-5\eta/12} \tag{3.1}$$

for some absolute constant $\eta > 0$.

Finally, we examine the case $R \gg q$. This time, we cover C with squares of side q, and observe that

$$\sum_{x,y \pmod q} \chi(Q(x,y)) = 0.$$

(By multiplicativity it suffices to prove this when q is prime, in which case it is an easy exercise, relying on the fact that Q is non-singular modulo q.) Since C will be partitioned into $O(R^2 q^{-2})$ complete squares and $O(Rq^{-1})$ partial squares we may use the result (3.1) to conclude that

$$\sum_{(x,y)\in C} \chi(Q(x,y)) \ll Rq^{-1} q^{2-5\eta/12} \leqslant R^{2-5\eta/12},$$

and the lemma follows.

We next estimate $\widehat{m}(Q;q)$ for binary forms Q.

LEMMA 3. *For any fixed $\delta > 0$,*

$$\widehat{m}(Q;q) \ll_{\delta} q^{1/4+\delta}$$

uniformly over odd square-free moduli q, and over binary forms Q subject to $(\det(Q), q) = 1$.

As already noted in the introduction, if we let d run over all divisors of q then, if $\sum_d \chi_d(m) > 0$, we must have $m \equiv t^2 \pmod q$ for some integer t. It follows that $\widehat{m}(Q;q) \leqslant R$ provided that

$$\sum_{d|q} \sum_{\|(x,y)\|\leqslant R} \chi_d(Q(x,y)) > 0.$$

https://doi.org/10.1112/S0025579315000364 Published online by Cambridge University Press

The number of divisors of q is $O_\varepsilon(q^\varepsilon)$, for any $\varepsilon > 0$. Choosing $\varepsilon = \eta/8$, it follows from Lemma 2 that if $R \geqslant q^{1/4+\delta}$, then

$$\sum_{d|q, d>1} \sum_{\|(x,y)\| \leqslant R} \chi_d(Q(x, y)) \ll_\delta R^{2-\eta} q^\varepsilon \ll R^{2-\eta/2}.$$

On the other hand,

$$\sum_{\|(x,y)\| \leqslant R} 1 \gg R^2,$$

and Lemma 3 follows.

Finally, we need to estimate $\widehat{B}_3(q)$ in terms of $\widehat{B}_2(q)$.

LEMMA 4. *We have*

$$\widehat{B}_3(q) \ll_\varepsilon q^\varepsilon \widehat{B}_2(q)$$

for any fixed $\varepsilon > 0$.

Once this is proved, we may deduce from Lemma 3 that $\widehat{B}_3(q) \ll_\varepsilon q^{1/4+\varepsilon}$ for any $\varepsilon > 0$, and hence Lemma 1 yields $B_3^*(q) \ll_\varepsilon q^{5/8+\varepsilon}$. This is the result required for Theorem 1.

To establish Lemma 4, we will find short vectors

$$(a_1, a_2), (a_3, a_4), (a_5, a_6) \in \mathbb{Z}^2 \tag{3.2}$$

such that the form

$$R(u, v) := Q(a_1u + a_2v, a_3u + a_4v, a_5u + a_6v) \tag{3.3}$$

has $(\det(R), q) = 1$. We can then choose $u, v \ll \widehat{B}_2(q)$, not both zero, such that $R(u, v)$ is a square modulo q, which will produce a corresponding vector

$$\mathbf{x} = (a_1u + a_2v, a_3u + a_4v, a_5u + a_6v)$$

for which $Q(\mathbf{x})$ is a square modulo q, and

$$\|\mathbf{x}\| \ll \|(u, v)\| \max(a_1, \ldots, a_6).$$

If $\mathbf{x}$ were to vanish, the three vectors (3.2) would all have to be proportional. But then the form (3.3) would have rank at most one, so that $\det(R) = 0$. This would contradict our assumption that $(\det(R), q) = 1$. It follows that $\mathbf{x} \neq \mathbf{0}$. Thus, to complete the proof of Lemma 4, it will suffice to show that we can choose the coefficients $a_1, \ldots, a_6$ to be of size $O_\varepsilon(q^\varepsilon)$.

Define

$$\Delta(a_1, \ldots, a_6) := \det(Q(a_1u + a_2v, a_3u + a_4v, a_5u + a_6v)).$$

This will be a sextic form in the six variables $a_1, \ldots, a_6$. We claim that for each prime factor p of q there is at least one choice of $\mathbf{a} \in \mathbb{Z}^6$ such that $p \nmid \Delta(\mathbf{a})$. Since we can diagonalize Q by a unimodular transformation over $\mathbb{F}_p$, a moment's reflection shows that it is enough to verify the claim when Q is a diagonal form. However, the result is trivial in this case, since $p \nmid \det(Q)$.

https://doi.org/10.1112/S0025579315000364 Published online by Cambridge University Press

We can now call on the following lemma, which we will prove shortly.

LEMMA 5. *Let $\varepsilon, \delta > 0$ be given. Suppose $F(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ is a form of degree d, and let $q \in \mathbb{N}$. Assume that for every prime divisor p of q there is at least one $\mathbf{a} \in \mathbb{Z}^n$ such that $p \nmid F(\mathbf{a})$. Then*

$$\#\{\mathbf{a} \in \mathbb{N}^n : \max a_i \leqslant A, (F(\mathbf{a}), q) = 1\} \gg_{d,n,\varepsilon,\delta} A^n q^{-\varepsilon}$$

as soon as $A \geqslant q^{\delta}$ and $q \gg_{n,d,\varepsilon,\delta} 1$.

This result shows that we have at least one vector $\mathbf{a}$ of size $\|\mathbf{a}\| \ll q^{\varepsilon}$ such that $\Delta(\mathbf{a})$ is coprime to q, which suffices to complete the proof.

It remains to prove Lemma 5. Define

$$N(e) := \#\{\mathbf{a} \pmod e : e \mid F(\mathbf{a})\}$$

for each $e \in \mathbb{N}$. Then $N(e)$ is multiplicative, and $N(p) < p^n$ for $p \mid q$, by the hypothesis of the lemma. Moreover, when $N(p) < p^n$ the form F cannot vanish identically modulo p, and hence $N(p) \ll_{d,n} p^{n-1}$. It follows that

$$N(e) \ll_{d,n,\eta} e^{n-1+\eta}$$

for $e \mid q$ and for any fixed $\eta > 0$.

We now consider

$$N(e, A) := \#\{\mathbf{a} \in \mathbb{N}^n : \max a_i \leqslant A, e \mid F(\mathbf{a})\}.$$

The set $(0, A]^n$ contains $[A/e]^n$ disjoint cubes of side-length e, and is included in a union of $(1 + [A/e])^n$ such cubes. It follows that

$$N(e, A) = \frac{A^n}{e^n} N(e) + O_n(A^{n-1} e^{1-n} N(e)) = \frac{A^n}{e^n} N(e) + O_{d,n,\eta}(A^{n-1} e^{\eta}) \quad (3.4)$$

when $e \mid q$ and $e \leqslant A$. To handle larger values of e, we use a rather general result of Browning and Heath-Brown [2]. For each $p_i \mid q$, let V_i be the affine variety over $\mathbb{F}_{p_i}$, given by $F = 0$. Since F does not vanish identically modulo p_i, this has dimension $n - 1$. We now apply [2, Lemma 4] with $W = \mathbb{A}^n$ and $k_i = n - 1$, for every index i. Taking $e \mid q$ with $e \geqslant A$, we find that there is a constant $C = C(d, n)$ such that

$$N(e, A) \ll C^{\omega(e)}(A^n e^{-1} + \omega(e) A^{n-1}) \ll_{d,n,\eta} e^{\eta} A^{n-1}$$

for any fixed $\eta > 0$. It follows that, if $e \geqslant A$,

$$\begin{aligned} N(e, A) &= \frac{A^n}{e^n} N(e) + O(A^n N(e) e^{-n}) + O_{d,n,\eta}(A^{n-1} e^{\eta}) \\ &= \frac{A^n}{e^n} N(e) + O_{d,n,\eta}(A^n e^{-1+\eta}) + O_{d,n,\eta}(A^{n-1} e^{\eta}) \\ &= \frac{A^n}{e^n} N(e) + O_{d,n,\eta}(A^{n-1} e^{\eta}), \end{aligned}$$

so that (3.4) holds whether $e \leqslant A$ or not.

https://doi.org/10.1112/S0025579315000364 Published online by Cambridge University Press

We now examine

$$\begin{aligned}
&\#\{\mathbf{a} \in \mathbb{N}^n : \max a_i \leqslant A, (F(\mathbf{a}), q) = 1\} \\
&\quad = \sum_{e|q} \mu(e) N(e, A) \\
&\quad = \sum_{e|q} \mu(e) \frac{A^n}{e^n} N(e) + O_{d,n,\eta}\left(\sum_{e|q} A^{n-1} e^{\eta}\right) \\
&\quad = A^n \prod_{p|q} (1 - N(p) p^{-n}) + O_{d,n,\eta}(A^{n-1} q^{2\eta}).
\end{aligned}$$

Since $N(p) < p^n$ and $N(p) \leqslant c_0 p^{n-1}$ for some constant c_0 depending only on d and n, we may deduce that

$$\begin{aligned}
\prod_{p|q} (1 - N(p) p^{-n}) &\geqslant \prod_{\substack{p|q \\ p \leqslant 2c_0}} (1 - (p^n - 1) p^{-n}) \prod_{\substack{p|q \\ p > 2c_0}} (1 - c_0 p^{-1}) \\
&\geqslant \prod_{p \leqslant 2c_0} p^{-n} \prod_{\substack{p|q \\ p > 2c_0}} (1 - p^{-1})^{2c_0} \\
&\gg_{d,n} \left(\frac{\phi(q)}{q}\right)^{2c_0} \\
&\gg_{d,n,\eta} q^{-\eta}.
\end{aligned}$$

It follows that

$$\#\{\mathbf{a} \in \mathbb{N}^n : \max a_i \leqslant A, (F(\mathbf{a}), q) = 1\} \geqslant c_2 A^n q^{-\eta} - c_3 A^{n-1} q^{2\eta}$$

for suitable positive constants c_2 and c_3 depending on η, d and n. The lemma then follows by taking $\eta = \min(\varepsilon, \delta/4)$.

§4. *Proof of Theorem 3.* For the proof we will write

$$\Sigma = \sum_{(x,y) \in C} \chi(Q(x, y))$$

for convenience. Let $N \in \mathbb{N}$ be a parameter to be chosen, satisfying $N \leqslant Rq^{-1/100}$, say, and set $S = [R/N]$. We need to specify a "good" set of vectors $\mathbf{s} \in \mathbb{N}^2$, and this will require a further definition. The form $Q(X, Y)$ should be thought of as lying in $(\mathbb{Z}/q\mathbb{Z})[X, Y]$, and we need an appropriate lift to $\mathbb{Z}[X, Y]$. To achieve this, we write $Q(x_1, x_2) = Ax_1^2 + Bx_1x_2 + Cx_2^2$ and

$$\Lambda = \{\mathbf{v} \in \mathbb{Z}^3 : \mathbf{v} \equiv \lambda(A, B, C) \pmod q \text{ for some } \lambda \in \mathbb{Z}\}, \tag{4.1}$$

and we let (A^*, B^*, C^*) be a non-zero vector in Λ of minimal length. As there is a non-zero vector $(A', B', C') \equiv (A, B, C) \pmod q$ in Λ with $|A'|, |B'|, |C'| \leqslant q/2$, we see that q cannot divide (A^*, B^*, C^*). We now define

$$Q^*(X, Y) = A^*X^2 + B^*XY + C^*Y^2.$$

https://doi.org/10.1112/S0025579315000364 Published online by Cambridge University Press

Note that $\det(Q^*) \equiv \lambda^2 \det(Q) \pmod q$ for an appropriate λ. Since q cannot divide λ and is square-free and coprime to $\det(Q)$, we will have $q \nmid \det(Q^*)$. In particular, Q^* is non-singular. (However we do not know that q and λ are coprime, and hence there is no guarantee that $(\det(Q^*), q) = 1$.) We can now take our set of "good" vectors $\mathbf{s}$ to be

$$\mathcal{S} = \{(s_1, s_2) \in \mathbb{N}^2 : \|\mathbf{s}\| \leqslant S, (Q(\mathbf{s}), q) = 1, Q^*(\mathbf{s}) \neq 0\}.$$

There are $O(S)$ vectors for which $Q^*(\mathbf{s}) = 0$, uniformly over all non-zero forms Q^*. Thus, according to Lemma 5,

$$\#\mathcal{S} \gg_\varepsilon S^2 q^{-\varepsilon}, \tag{4.2}$$

for $S \gg_\varepsilon q^\varepsilon$, for any fixed $\varepsilon > 0$.

For any positive integer $n \leqslant N$ we proceed to write

$$(\#\mathcal{S})\Sigma = \sum_{(s_1,s_2)\in\mathcal{S}} \sum_{(x_1,x_2)\in\mathbb{Z}^2} \chi(Q(x_1 + ns_1, x_2 + ns_2)) \mathbb{1}_C(x_1 + ns_1, x_2 + ns_2),$$

where $\mathbb{1}_C$ is the characteristic function for the set C. It follows that

$$N(\#\mathcal{S})\Sigma = \sum_{(s_1,s_2)\in\mathcal{S}} \sum_{(x_1,x_2)\in\mathbb{Z}^2} \sum_{n\in I} \chi(Q(x_1 + ns_1, x_2 + ns_2)),$$

where

$$I = \{n \leqslant N : (x_1 + ns_1, x_2 + ns_2) \in C\}.$$

Since C is convex, I is an interval. Moreover, if I is non-empty, containing $\mathbf{x}+n\mathbf{s}$, then $\|\mathbf{x} + n\mathbf{s} - \mathbf{x}_0\| \leqslant R$ and $\|n\mathbf{s}\| \leqslant NS \leqslant R$, and hence $\|\mathbf{x} - \mathbf{x}_0\| \leqslant 2R$. We therefore deduce, via (4.2), that

$$\Sigma \ll_\varepsilon N^{-1} S^{-2} q^\varepsilon \sum_{\mathbf{s}\in\mathcal{S}} \sum_{\substack{\mathbf{x}\in\mathbb{Z}^2 \\ \|\mathbf{x}-\mathbf{x}_0\|\leqslant 2R}} \max_{I\subseteq(0,N]} \left| \sum_{n\in I} \chi(Q(x_1 + ns_1, x_2 + ns_2)) \right|.$$

If the reader compares this with the corresponding stage in the argument of Chang [7] (see [7, (4.3)]), for example, then it will be observed that Chang has a product st in place of our variable n. Indeed, our method is slightly different from Chang's, as it requires one fewer variable and does not use an argument corresponding to [7, Lemma 3].

To proceed further we use the readily verified identity

$$Q(x_1 + ns_1, x_2 + ns_2) = Q(\mathbf{s})\widetilde{Q}(n + a(\mathbf{s}, \mathbf{x}), b(\mathbf{s}, \mathbf{x})),$$

where $\widetilde{Q}(x_1, x_2) := x_1^2 + Bx_1x_2 + ACx_2^2$, and

$$a(\mathbf{s}, \mathbf{x}) = \frac{Ax_1s_1 + Bx_1s_2 + Cx_2s_2}{Q(s_1, s_2)}, \qquad b(\mathbf{s}, \mathbf{x}) = \frac{x_2s_1 - x_1s_2}{Q(s_1, s_2)}. \tag{4.3}$$

https://doi.org/10.1112/S0025579315000364 Published online by Cambridge University Press

Here the fractions are to be interpreted in the ring $\mathbb{Z}/q\mathbb{Z}$, the denominators $Q(s_1, s_2)$ being units by our choice of the set $\mathcal{S}$. We now write

$$N(a,b) = \#\{(\mathbf{s},\mathbf{x}) \in \mathcal{S}\times\mathbb{Z}^2 : \|\mathbf{x}-\mathbf{x}_0\| \leqslant 2R, a(\mathbf{s},\mathbf{x}) = a, b(\mathbf{s},\mathbf{x}) = b\},$$

and hence

$$\Sigma \ll_\varepsilon N^{-1}S^{-2}q^\varepsilon \sum_{a,b \pmod q} N(a,b) \max_{I\subseteq(0,N]}\left|\sum_{n\in I}\chi(\widetilde{Q}(n+a,b))\right|.$$

We must now consider the mean square of $N(a,b)$, for which we will prove the following bound.

LEMMA 6. *For any fixed $\varepsilon > 0$,*

$$\sum_{a,b \pmod q} N(a,b)^2 \ll_\varepsilon q^\varepsilon R^2S^2(1 + RSq^{-1/2} + R^2S^2q^{-4/3}).$$

This will be established in the next section.

We also have the trivial bound

$$\sum_{a,b \pmod q} N(a,b) \leqslant \#\{(\mathbf{s},\mathbf{x}) \in \mathcal{S}\times\mathbb{Z}^2 : \|\mathbf{x}-\mathbf{x}_0\| \leqslant 2R\} \ll R^2S^2,$$

and hence Hölder's inequality yields

$$\begin{aligned}\Sigma^{2r} &\ll_{\varepsilon,r} (N^{-1}S^{-2}q^\varepsilon)^{2r}\left\{\sum_{a,b \pmod q} N(a,b)\right\}^{2r-2}\left\{\sum_{a,b \pmod q} N(a,b)^2\right\}\\ &\quad\times \sum_{a,b \pmod q}\max_{I\subseteq(0,N]}\left|\sum_{n\in I}\chi(\widetilde{Q}(n+a,b))\right|^{2r}\\ &\ll_{\varepsilon,r} N^{-2r}R^{4r-2}S^{-2}q^\varepsilon(1 + RSq^{-1/2} + R^2S^2q^{-4/3})\\ &\quad\times \sum_{a,b \pmod q}\max_{I\subseteq(0,N]}\left|\sum_{n\in I}\chi(\widetilde{Q}(n+a,b))\right|^{2r}\\ &\ll_{\varepsilon,r} N^{2-2r}R^{4r-4}q^\varepsilon(1 + R^2N^{-1}q^{-1/2} + R^4N^{-2}q^{-4/3})\\ &\quad\times \sum_{a,b \pmod q}\max_{I\subseteq(0,N]}\left|\sum_{n\in I}\chi(\widetilde{Q}(n+a,b))\right|^{2r}, \end{aligned} \tag{4.4}$$

on employing our convention concerning the values taken by ε.

We are therefore led to consider sums of the form

$$S(q;H) := \sum_{a,b \pmod q}\left|\sum_{n\leqslant H}\chi(\widetilde{Q}(n+a,b))\right|^{2r}.$$

https://doi.org/10.1112/S0025579315000364 Published online by Cambridge University Press

To estimate these, we expand to obtain

$$S(q; H) = \sum_{n_1,\dots,n_{2r} \leqslant H} \Sigma(q; \mathbf{n})$$

with

$$\Sigma(q; \mathbf{n}) = \sum_{a,b \pmod q} \chi(F_+(a, b; \mathbf{n}))\overline{\chi}(F_-(a, b; \mathbf{n}))$$

and

$$F_+(X, Y; \mathbf{n}) = \prod_{i=1}^{r} \widetilde{Q}(n_i + X, Y), \qquad F_-(X, Y; \mathbf{n}) = \prod_{i=r+1}^{2r} \widetilde{Q}(n_i + X, Y).$$

The sums $\Sigma(q; \mathbf{n})$ have a standard multiplicative property. If $q = uv$, say, then u and v will be coprime and square-free, and we can write $\chi = \chi_u \chi_v$ for suitable primitive characters to moduli u and v, respectively. Then

$$\Sigma(q; \mathbf{n}) = \Sigma(u; \mathbf{n})\Sigma(v; \mathbf{n}). \tag{4.5}$$

It therefore suffices to understand $\Sigma(q; \mathbf{n})$ when q is prime, for which we have the following result.

LEMMA 7. *Let p be an odd prime not dividing* $\det(\widetilde{Q})$*, and let χ be a non-principal character to modulus p. Write*

$$\Delta_i = \prod_{\substack{1 \leqslant j \leqslant 2r \\ j \neq i}} (n_j - n_i)$$

and

$$\Delta = \text{h.c.f.}(\Delta_1, \dots, \Delta_{2r}).$$

Then

$$|\Sigma(p; \mathbf{n})| \leqslant 4r^2 p(p, \Delta).$$

We will prove this in §6. By summing over the $(2r)$-tuples $\mathbf{n}$ we are then able to establish the following bound for $S(q; H)$.

LEMMA 8. *For any $\varepsilon > 0$ and $r \in \mathbb{N}$,*

$$S(q, H) \ll_{\varepsilon, r} (qH)^{\varepsilon}(qH^{2r} + q^2 H^r).$$

This will be proved in §7.

Having established this, there is a standard procedure to insert a maximum over subintervals of $(0, N]$, which goes back to Rademacher [**15**] and Menchov [**14**]. We do not repeat the details, but instead refer the reader to Gallager and Montgomery [**9**, §3] or Heath-Brown [**13**, §2]. The outcome is the following result.

https://doi.org/10.1112/S0025579315000364 Published online by Cambridge University Press

LEMMA 9. *For any $\varepsilon > 0$ and $r \in \mathbb{N}$,*

$$\sum_{a,b \pmod q} \max_{I \subseteq (0,N]} \left| \sum_{n \in I} \chi(\widetilde{Q}(n+a,b)) \right|^{2r} \ll_{\varepsilon,r} (qN)^{\varepsilon}(qN^{2r} + q^2N^r).$$

We are now ready to complete the proof of Theorem 3. We insert the bound of Lemma 9 into (4.4), to give

$$\begin{aligned}\Sigma^{2r} \ll_{\varepsilon,r} & N^{2-2r}R^{4r-4}q^{\varepsilon}(1 + R^2N^{-1}q^{-1/2} + R^4N^{-2}q^{-4/3}) \\ & \cdot (qN)^{\varepsilon}(qN^{2r} + q^2N^r).\end{aligned}$$

In order to balance the final two terms, we choose $N = [q^{1/r}]$, which satisfies our constraint $N \leqslant Rq^{-1/100}$ provided that $R \geqslant q^{1/4+1/2r}$ and $r \geqslant 3$. On redefining ε we then find that

$$\begin{aligned}\Sigma^{2r} &\ll_{\varepsilon,r} q^{\varepsilon}N^{2-2r}R^{4r-4}(1 + R^2N^{-1}q^{-1/2} + R^4N^{-2}q^{-4/3}) \cdot qN^{2r} \\ &\ll_{\varepsilon,r} q^{1/2+1/r+\varepsilon}R^{4r-2}(R^{-2}q^{1/2+1/r} + 1 + R^2q^{-5/6-1/r}),\end{aligned}$$

and the theorem follows.

§5. *Proof of Lemma 6.* We now prove Lemma 6. In view of the definitions (4.3) we have the identity

$$(Ab(\mathbf{s},\mathbf{x})X - a(\mathbf{s},\mathbf{x})Y)(s_2X - s_1Y) = s_2b(\mathbf{s},\mathbf{x})Q(X,Y) - (x_2X - x_1Y)Y$$

in $(\mathbb{Z}/q\mathbb{Z})[X,Y]$. Thus, if $a(\mathbf{s},\mathbf{x}) = a(\mathbf{s}',\mathbf{x}') = a$ and $b(\mathbf{s},\mathbf{x}) = b(\mathbf{s}',\mathbf{x}') = b$, then

$$\begin{aligned}&(AbX - aY)(s_2X - s_1Y)(s_2'X - s_1'Y) \\ &\quad = (s_2bQ(X,Y) - (x_2X - x_1Y)Y)(s_2'X - s_1'Y),\end{aligned}$$

and also

$$\begin{aligned}&(AbX - aY)(s_2'X - s_1'Y)(s_2X - s_1Y) \\ &\quad = (s_2'bQ(X,Y) - (x_2'X - x_1'Y)Y)(s_2X - s_1Y).\end{aligned}$$

Thus, by subtraction, we deduce that

$$\begin{aligned}&Y\{(x_2X - x_1Y)(s_2'X - s_1'Y) - (x_2'X - x_1'Y)(s_2X - s_1Y)\} \\ &\quad = b(s_2's_1 - s_1's_2)YQ(X,Y),\end{aligned}$$

still in $(\mathbb{Z}/q\mathbb{Z})[X,Y]$.

We then deduce that

$$(x_2s_2' - x_2's_2, x_2's_1 + x_1's_2 - x_2s_1' - x_1s_2', x_1s_1' - x_1's_1) \in \Lambda, \tag{5.1}$$

with Λ given by (4.1). It follows that

$$\sum_{a,b} N(a,b)^2 \leqslant \sum_{\mathbf{s},\mathbf{s}' \in \mathcal{S}} N_1(\mathbf{s},\mathbf{s}'),$$

https://doi.org/10.1112/S0025579315000364 Published online by Cambridge University Press

where $N_1(\mathbf{s}, \mathbf{s}')$ counts pairs of vectors $(\mathbf{x}, \mathbf{x}')$ each lying in the disc $\|\mathbf{x} - \mathbf{x}_0\| \leqslant 2R$, such that (5.1) holds. Now suppose that $(\mathbf{x}_1, \mathbf{x}_1')$ is a pair counted by $N_1(\mathbf{s}, \mathbf{s}')$. For any other such pair we write $\mathbf{x} = \mathbf{x}_1 + \mathbf{u}$ and $\mathbf{x}' = \mathbf{x}_1' + \mathbf{u}'$ and hence, by subtraction, we find, firstly, that $\|\mathbf{u}\|, \|\mathbf{u}'\| \leqslant 4R$ and, secondly, that

$$(u_2 s_2' - u_2' s_2, u_2' s_1 + u_1' s_2 - u_2 s_1' - u_1 s_2', u_1 s_1' - u_1' s_1) \in \Lambda. \tag{5.2}$$

Thus $N_1(\mathbf{s}, \mathbf{s}') \leqslant N_2(\mathbf{s}, \mathbf{s}')$, where $N_2(\mathbf{s}, \mathbf{s}')$ counts pairs of vectors $\mathbf{u}, \mathbf{u}'$ satisfying (5.2), and having length at most $4R$.

We have already chosen $(A^*, B^*, C^*) = \mathbf{v}_1$, say, as the shortest vector in Λ. As in the proof of Davenport [**8**, Lemma 5], we can then construct a basis $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ for Λ, such that if $\mathbf{v} = \lambda_1 \mathbf{v}_1 + \lambda_2 \mathbf{v}_2 + \lambda_3 \mathbf{v}_3$, then $\lambda_i \ll \|\mathbf{v}\| / \|\mathbf{v}_i\|$ for $i = 1, 2, 3$. Moreover,

$$\|\mathbf{v}_1\| \leqslant \|\mathbf{v}_2\| \leqslant \|\mathbf{v}_3\|$$

and

$$\|\mathbf{v}_1\| \cdot \|\mathbf{v}_2\| \cdot \|\mathbf{v}_3\| \geqslant \det(\Lambda).$$

In our case, $\det(\Lambda) = q^2$, and hence

$$\|\mathbf{v}_2\| \cdot \|\mathbf{v}_3\| \geqslant q^{4/3}.$$

In addition, one sees from the definition of Λ that $q \mid \mathbf{v}_1 \wedge \mathbf{v}_2$ and, since the vectors $\mathbf{v}_1$ and $\mathbf{v}_2$ are not proportional, it follows that

$$q \leqslant \|\mathbf{v}_1 \wedge \mathbf{v}_2\| \leqslant \|\mathbf{v}_1\| \cdot \|\mathbf{v}_2\| \leqslant \|\mathbf{v}_2\|^2.$$

The vector

$$\mathbf{v} = (u_2 s_2' - u_2' s_2, u_2' s_1 + u_1' s_2 - u_2 s_1' - u_1 s_2', u_1 s_1' - u_1' s_1)$$

has length at most $32RS$ so that the corresponding coefficients satisfy

$$\lambda_2 \ll \frac{RS}{\|\mathbf{v}_2\|} \quad \text{and} \quad \lambda_3 \ll \frac{RS}{\|\mathbf{v}_3\|}.$$

If we break the available vectors counted by $N_2(\mathbf{s}, \mathbf{s}')$ into subsets according to the values of λ_2 and λ_3, then the number of such subsets will be

$$\ll \left(1 + \frac{RS}{\|\mathbf{v}_2\|}\right)\left(1 + \frac{RS}{\|\mathbf{v}_3\|}\right) \ll 1 + \frac{RS}{\|\mathbf{v}_2\|} + \frac{R^2S^2}{\|\mathbf{v}_2\| \cdot \|\mathbf{v}_3\|} \ll 1 + \frac{RS}{q^{1/2}} + \frac{R^2S^2}{q^{4/3}}.$$

If $(\mathbf{u}_1, \mathbf{u}_1')$ and $(\mathbf{u}_2, \mathbf{u}_2')$ are two pairs belonging to the same subset and we write $\mathbf{u} = \mathbf{u}_1 - \mathbf{u}_2$ and $\mathbf{u}' = \mathbf{u}_1' - \mathbf{u}_2'$, then

$$\mathbf{v} = (u_2 s_2' - u_2' s_2, u_2' s_1 + u_1' s_2 - u_2 s_1' - u_1 s_2', u_1 s_1' - u_1' s_1) \tag{5.3}$$

will be a multiple of $\mathbf{v}_1 = (A^*, B^*, C^*)$, and we will have $\|\mathbf{u}\|, \|\mathbf{u}'\| \leqslant 8R$.

https://doi.org/10.1112/S0025579315000364 Published online by Cambridge University Press

We therefore conclude that

$$N_2(\mathbf{s}, \mathbf{s}') \ll (1 + RSq^{-1/2} + R^2S^2q^{-4/3})N_3(\mathbf{s}, \mathbf{s}'),$$

where $N_3(\mathbf{s}, \mathbf{s}')$ counts pairs of vectors $\mathbf{u}, \mathbf{u}'$ having length at most $8R$ and for which the vector (5.3) is an integer multiple of (A^*, B^*, C^*). The quadratic form corresponding to $\mathbf{v}$ is

$$\begin{aligned}(u_2s_2' - u_2's_2)X^2 + (u_2's_1 + u_1's_2 - u_2s_1' - u_1s_2')XY + (u_1s_1' - u_1's_1)Y^2 \\ = (u_2X - u_1Y)(s_2'X - s_1'Y) - (u_2'X - u_1'Y)(s_2X - s_1Y).\end{aligned}$$

We therefore conclude that

$$Q^*(X, Y) \mid (u_2X - u_1Y)(s_2'X - s_1'Y) - (u_2'X - u_1'Y)(s_2X - s_1Y). \tag{5.4}$$

Thus, to complete the proof of Lemma 6, it suffices to show that

$$\begin{aligned}\#\{(\mathbf{u}, \mathbf{u}', \mathbf{s}, \mathbf{s}') \in \mathbb{Z}^2 \times \mathbb{Z}^2 \times \mathcal{S} \times \mathcal{S} : \|\mathbf{u}\|, \|\mathbf{u}'\| \leqslant 8R, \ (5.4) \text{ holds}\} \\ \ll_\varepsilon q^\varepsilon R^2S^2.\end{aligned} \tag{5.5}$$

Given two binary quadratic forms Q_1 and Q_2, one may define a covariant $C(Q_1, Q_2)$ as the discriminant of the binary form $D(\alpha, \beta) = \det(\alpha Q_1 + \beta Q_2)$. One readily confirms that $C(Q_1, Q_2) = C(Q_1 + \lambda Q_2, Q_2)$ for any constant λ, and, moreover, that

$$C((u_2X - u_1Y)(v_2X - v_1Y), Q) = Q(u_1, u_2)Q(v_1, v_2).$$

Taking $Q_1 = (u_2X - u_1Y)(s_2'X - s_1'Y)$ and $Q_2 = Q^*$, we deduce that

$$Q^*(u_1, u_2)Q^*(s_1', s_2') = Q^*(u_1', u_2')Q^*(s_1, s_2). \tag{5.6}$$

In defining the set $\mathcal{S}$, we arranged that $Q^*(\mathbf{s}) \neq 0$. If $Q^*(\mathbf{u}) \neq 0$, it follows that $Q^*(u_1, u_2)Q^*(s_1', s_2')$ has $O_\varepsilon(q^\varepsilon)$ divisors, since

$$|Q^*(u_1, u_2)Q^*(s_1', s_2')| \ll \max(|A^*|, |B^*|, |C^*|)^2\|\mathbf{u}\|^2\|\mathbf{s}\|^2 \ll q^2R^2S^2 \ll q^6.$$

Moreover, when $d \neq 0$ the equation $Q^*(u_1', u_2') = d$ will have $\ll_\varepsilon (qR)^\varepsilon \ll_\varepsilon q^\varepsilon$ solutions $\mathbf{u}'$ with $\|\mathbf{u}'\| \leqslant 8R$ by, for example, Theorem 13 of Heath-Brown [12]. (Here we crucially use the fact that Q^* is non-singular.) Similarly, $Q^*(s_1, s_2) = d'$ will have $O_\varepsilon(q^\varepsilon)$ solutions for any $d' \neq 0$. It then follows that the contribution arising from 4-tuples $(\mathbf{u}, \mathbf{u}', \mathbf{s}, \mathbf{s}')$, in which $Q^*(\mathbf{u}) \neq 0$, will be $O_\varepsilon(q^\varepsilon R^2S^2)$, which is satisfactory for (5.5).

It remains to deal with the case in which $Q^*(\mathbf{u}) = 0$. In view of (5.6), we will then have $Q^*(\mathbf{u}') = 0$, since $Q^*(\mathbf{s})$ and $Q^*(\mathbf{s}')$ are non-zero. We now claim that either $\mathbf{u} = \mathbf{u}' = \mathbf{0}$, or $Q^*(X, Y)$ factors over $\mathbb{Z}$ into linear factors $L_1(X, Y)$ and $L_2(X, Y)$ such that $L_1(X, Y)$ divides both $u_2X - u_1Y$ and $u_2'X - u_1'Y$. To see this, suppose that $\mathbf{u} \neq \mathbf{0}$, say. Then we must have $L_1(X, Y) \mid u_2X - u_1Y$ for

https://doi.org/10.1112/S0025579315000364 Published online by Cambridge University Press

some integral linear factor of Q^*. It would then follow, from (5.4), that $L_1(X, Y) \mid u_2'X - u_1'Y$, since $Q^*(\mathbf{s}) \neq 0$. The claim then follows.

Clearly, the contribution to (5.5) arising from the case $\mathbf{u} = \mathbf{u}' = \mathbf{0}$ is $O(S^4) = O(R^2S^2)$, which is satisfactory, so it remains to consider the case in which

$$u_2X - u_1Y = kL_1(X, Y) \quad \text{and} \quad u_2'X - u_1'Y = k'L_1(X, Y)$$

with integers k, k' such that $|k|, |k'| \leqslant 8R$. We then have

$$k(s_2'X - s_1'Y) \equiv k'(s_2X - s_1Y) \pmod{L_2(X, Y)},$$

by (5.4). If $L_2(X, Y) = aX - bY$, say, then we must have

$$k(s_2'b - s_1'a) = k'(s_2b - s_1a).$$

Moreover, $s_2'b - s_1'a$ and $s_2b - s_1a$ are non-zero, since $Q^*(\mathbf{s})$ and $Q^*(\mathbf{s}')$ do not vanish. If $k' = 0$, then $k = 0$, which would put us in the case $\mathbf{u} = \mathbf{u}' = \mathbf{0}$, which has already been dealt with. Since at most one of a or b can vanish, we may suppose that b, say, is non-zero. There are then $O(RS^3)$ possibilities for s_1', s_1, s_2 and k', and the number of divisors k of $k'(s_2b - s_1a)$ will be $O_\varepsilon((qS)^\varepsilon)$, since $|a|, |b| \ll \max(|A^*|, |B^*|, |C^*|) \ll q$. The complementary divisor to k is then $s_2'b - s_1'a$, which determines s_2'. We therefore conclude that the corresponding contribution to (5.5) is $O_\varepsilon(q^\varepsilon R^2S^2)$, since $S \leqslant R \leqslant q$. This completes the proof of (5.5), and hence of Lemma 6.

§6. *Proof of Lemma 7.* Our proof of Lemma 7 is inspired by the viewpoint of Chang [7]. We first consider the case in which $\widetilde{Q}(X, Y) = X^2 + BXY + ACY^2$ factors modulo p. In this case, we may replace $\widetilde{Q}(X, Y)$ by $(X + \lambda Y)(X + \mu Y)$, say, where $p \nmid \lambda - \mu$, since $p \nmid \det(\widetilde{Q})$. Then $\widetilde{Q}(n + a, b) = (n + a')(n + b')$, where $a' = a + \lambda b$ and $b' = a + \mu b$ are independent of n. Moreover, (a', b') runs over $\mathbb{F}_p^2$ as (a, b) does. It follows that

$$\Sigma(p; \mathbf{n}) = \sum_{a,b \pmod p} \chi(G_+(a, b; \mathbf{n}))\overline{\chi}(G_-(a, b; \mathbf{n}))$$

with

$$G_+(X, Y; \mathbf{n}) = \prod_{i=1}^{r}(n_i+X)(n_i+Y), \qquad G_-(X, Y; \mathbf{n}) = \prod_{i=r+1}^{2r}(n_i+X)(n_i+Y).$$

We then see that

$$\Sigma(p; \mathbf{n}) = \Sigma_1(p; \mathbf{n})^2$$

with

$$\Sigma_1(p; \mathbf{n}) = \sum_{a \pmod p} \chi(H_+(a; \mathbf{n}))\overline{\chi}(H_-(a; \mathbf{n}))$$

https://doi.org/10.1112/S0025579315000364 Published online by Cambridge University Press

and

$$H_+(X;\mathbf{n}) = \prod_{i=1}^{r}(n_i + X), \qquad H_-(X;\mathbf{n}) = \prod_{i=r+1}^{2r}(n_i + X).$$

The sum $\Sigma_1(p;\mathbf{n})$ occurs in the work of Burgess [3, Lemma 1], from which one readily sees that

$$|\Sigma_1(p;\mathbf{n})| \leqslant 2r\sqrt{p}, \tag{6.1}$$

unless every linear factor of the polynomial $H_+(X;\mathbf{n})H_-(X;\mathbf{n})$ has multiplicity two or more, modulo p. In the exceptional case, $p \mid \Delta_i$ for every i, and hence $p \mid \Delta$. We deduce that (6.1) holds whenever $p \nmid \Delta$. In the remaining case, we have a trivial bound $|\Sigma_1(p;\mathbf{n})| \leqslant p$, so that

$$|\Sigma_1(p;\mathbf{n})| \leqslant 2rp^{1/2}(p,\Delta)^{1/2}$$

whether or not $p \nmid \Delta$. We therefore conclude that

$$|\Sigma(p;\mathbf{n})| \leqslant 4r^2 p(p,\Delta)$$

whenever $\widetilde{Q}$ factors modulo p. This is satisfactory for Lemma 7.

We turn now to the case in which $\widetilde{Q}$ is irreducible over $\mathbb{F}_p$. It will be typographically convenient to write F for the field $\mathbb{F}_{p^2}$. In the case under consideration, there is a factorization $\widetilde{Q}(X,Y) = (X+\lambda Y)(X+\lambda' Y)$, say, over F with λ and λ' being conjugates in $F/\mathbb{F}_p$. We may now define a function ψ from F to $\mathbb{C}$ by setting

$$\psi(a+\lambda b) = \chi((a+\lambda b)(a+\lambda' b)) = \chi(\widetilde{Q}(a,b)).$$

One easily sees that this is a non-trivial multiplicative character on F, and that

$$\Sigma(p;\mathbf{n}) = \sum_{\alpha\in F} \psi(H_+(\alpha;\mathbf{n}))\overline{\psi}(H_-(\alpha;\mathbf{n})).$$

Burgess' proof of (6.1), based on Weil's "Riemann Hypothesis" for curves over arbitrary finite fields, immediately extends to $\Sigma(p;\mathbf{n})$, and shows that

$$|\Sigma(p;\mathbf{n})| \leqslant 2r\sqrt{\#F} = 2rp,$$

unless every linear factor of the polynomial $H_+(X;\mathbf{n})H_-(X;\mathbf{n})$ has multiplicity two or more, modulo p. In the alternative case, we have $p \mid \Delta$, in the notation of the lemma, and we deduce that

$$|\Sigma(p;\mathbf{n})| \leqslant p(p,\Delta),$$

in view of the trivial bound $|\Sigma(p;\mathbf{n})| \leqslant p^2$. As above, these bounds are satisfactory for Lemma 7.

https://doi.org/10.1112/S0025579315000364 Published online by Cambridge University Press

§7. *Proof of Lemma 8.* It follows from Lemma 7, along with the multiplicative relation (4.5), that

$$\Sigma(q; \mathbf{n}) \leqslant (4r^2)^{\omega(q)} q(q, \Delta) \ll_{\varepsilon,r} q^{1+\varepsilon}(q, \Delta).$$

Thus, to prove Lemma 8, it will be enough to show that

$$\sum_{n_1,\dots,n_{2r} \leqslant H} (q, \Delta) \ll_{\varepsilon,r} (qH)^{\varepsilon}(H^{2r} + qH^r).$$

Indeed,

$$\sum_{n_1,\dots,n_{2r} \leqslant H} (q, \Delta) \leqslant \sum_{k|q} k\#\{\mathbf{n} \in \mathbb{N}^{2r} \cap (0, H]^{2r} : k \mid \Delta\},$$

so that it suffices to establish the estimate

$$\#\{\mathbf{n} \in \mathbb{N}^{2r} \cap (0, H]^{2r} : k \mid \Delta\} \ll_{\varepsilon,r} (kH)^{\varepsilon}(H^{2r}k^{-1} + H^r). \tag{7.1}$$

We first consider vectors $\mathbf{n}$ for which $\Delta_1 = \cdots = \Delta_{2r} = 0$. Then if $\nu \in \mathbb{N}$ and there is any index i such that $n_i = \nu$, there must be at least two such indices. It follows that the set $\{n_1, \dots, n_{2r}\}$ contains at most r distinct elements. There are at most H^r choices for these elements, $\nu_1, \dots, \nu_s$, say, with $1 \leqslant s \leqslant r$. Once the ν_j have been chosen, there are (at most) s choices for each n_i. It follows that there are $O_r(H^r)$ vectors $\mathbf{n}$ for which $\Delta_1 = \cdots = \Delta_{2r} = 0$. This is satisfactory for (7.1).

In the remaining case, $\Delta_j \neq 0$ for some index j, and

$$\begin{aligned}\#\{\mathbf{n} \in \mathbb{N}^{2r} \cap (0, H]^{2r} : k \mid \Delta, \Delta \neq 0\} \\ \leqslant \sum_{j=1}^{2r} \#\{\mathbf{n} \in \mathbb{N}^{2r} \cap (0, H]^{2r} : k \mid \Delta_j, \Delta_j \neq 0\}.\end{aligned}$$

However, $|\Delta_j| \leqslant H^{2r-1}$, so that there are at most $2H^{2r-1}k^{-1}$ possibilities for Δ_j. For each such choice of Δ_j, there are at most $2d(|\Delta_j|) \ll_{\varepsilon,r} H^{\varepsilon}$ possibilities for each of its divisors $n_i - n_j$. Thus, taking account of the $O(H)$ possibilities for n_j itself, we find that

$$\#\{\mathbf{n} \in \mathbb{N}^{2r} \cap (0, H]^{2r} : k \mid \Delta_j, \Delta_j \neq 0\} \ll_{\varepsilon,r} H^{2r-1}k^{-1}(H^{\varepsilon})^{2r-1}H.$$

After replacing ε by $\varepsilon/(2r-1)$, we see that this is $O_{\varepsilon,r}(H^{2r+\varepsilon}k^{-1})$. Since this is satisfactory for (7.1), the proof of Lemma 8 is complete.

Acknowledgement. This research was supported by EPSRC grant EP/K0211-32X/1.

https://doi.org/10.1112/S0025579315000364 Published online by Cambridge University Press

References

1. R. C. Baker, *Diophantine Inequalities* (*London Mathematical Society Monographs New Series* **1**) (Oxford University Press, Oxford, 1986).
2. T. D. Browning and D. R. Heath-Brown, Rational points on quartic hypersurfaces. *J. Reine Angew. Math.* **629** (2009), 37–88.
3. D. A. Burgess, On character sums and primitive roots. *Proc. Lond. Math. Soc.* (3) **12** (1962), 179–192.
4. D. A. Burgess, On character sums and L-series. II. *Proc. Lond. Math. Soc.* (3) **13** (1963), 524–536.
5. D. A. Burgess, On the quadratic character of a polynomial. *J. Lond. Math. Soc.* **42** (1967), 73–80.
6. D. A. Burgess, A note on character sums of binary quadratic forms. *J. Lond. Math. Soc.* **43** (1968), 271–274.
7. M.-C. Chang, Burgess inequality in $\mathbb{F}_{p^2}$. *Geom. Funct. Anal.* **19** (2009), 1001–1016.
8. H. Davenport, Cubic forms in sixteen variables. *Proc. R. Soc. Lond. Ser. A* **272** (1963), 285–303.
9. P. X. Gallagher and H. L. Montgomery, On the Burgess estimate. *Math. Notes* **88** (2010), 321–329.
10. D. R. Heath-Brown, Small solutions of quadratic congruences. *Glasg. Math. J.* **27** (1985), 87–93.
11. D. R. Heath-Brown, Small solutions of quadratic congruences, II. *Mathematika* **38**(2) (1992), 264–284.
12. D. R. Heath-Brown, The density of rational points on cubic surfaces. *Acta Arith.* **79** (1997), 17–30.
13. D. R. Heath-Brown, Burgess's bounds for character sums. In *Number Theory and Related Fields* (*Springer Proceedings in Mathematics & Statistics* **43**), Springer (New York, 2013), 199–213.
14. D. Menchov, Sur les séries de fonctions orthogonales. *Fund. Math.* **1** (1923), 82–105.
15. H. Rademacher, Einige Sätze über Reihen von allgemeinen Orthogonal-Funktionen. *Math. Ann.* **87** (1922), 112–138.
16. A. Schinzel, H.-P. Schlickewei and W. M. Schmidt, Small solutions of quadratic congruences and small fractional parts of quadratic forms. *Acta Arith.* **37** (1980), 241–248.

D. R. Heath-Brown,
Mathematical Institute,
Radcliffe Observatory Quarter,
Woodstock Road,
Oxford OX2 6GG,
U.K.
E-mail: rhb@maths.ox.ac.uk

https://doi.org/10.1112/S0025579315000364 Published online by Cambridge University Press