SMALL SOLUTIONS OF QUADRATIC CONGRUENCES

by D. R. HEATH-BROWN

To Robert Rankin on the occasion of his 70th birthday

1. Introduction. Let $Q(\mathbf{x}) = Q(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ be a quadratic form. We investigate the size of the smallest non-zero solution of the congruence $Q(\mathbf{x}) \equiv 0 \pmod{q}$. We seek a bound $B_n(q)$, independent of Q, such that there is always a non-zero solution satisfying

$$\operatorname*{Max}_{1 \leq i \leq n} |x_i| \leq B_n(q).$$

The form $Q(\mathbf{x}) = \sum_i^n x_i^2$ gives the trivial lower bound $B_n(q) \geq (q/n)^{1/2}$ for all q and n, since if $\mathbf{x} \neq \mathbf{0}$ and $q \mid Q(\mathbf{x})$, then $Q(\mathbf{x}) \geq q$.

It was shown by Schinzel, Schlickewei and Schmidt [**3**] that

$$B_n(q) \leq q^{1/2 + 1/(4[(n-1)/2]+2)}, \qquad (n \geq 3). \tag{1}$$

They used this to obtain Diophantine approximation results for $\|Q(\mathbf{x})\|$, in which Q is a quadratic form with real coefficients. It is reasonable to conjecture that

$$B_n(q) \ll q^{1/2+\varepsilon}, \tag{2}$$

for any $\varepsilon > 0$, as soon as $n \geq 4$, but no general improvement on (1) is known. However we shall show that the above conjecture is indeed true if q is restricted to prime values.

THEOREM 1. *We have $B_n(p) \ll p^{1/2}(\log p)$ uniformly for $n \geq 4$, where p is prime.*

Indeed using the method of [**3**] we shall easily prove a stronger result in certain cases.

THEOREM 2. *Let p be an odd prime and take $n = 4$. If $p \mid \det Q$ or $\left(\frac{\det Q}{p}\right) = 1$ then $p \mid Q(\mathbf{x})$ for some $\mathbf{x} \in \mathbb{Z}^4 - \{\mathbf{0}\}$, with* $\operatorname{Max} |x_i| \leq p^{1/2}$.

Here $\det Q$ is the determinant of the integer matrix representing Q, and $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol.

The condition $n \geq 4$ in Theorem 1, and in the general conjecture (2), is in fact necessary. Indeed if $n = 3$ the bound (1) is essentially best possible, even when q is restricted to be prime.

THEOREM 3. *For all primes p we have $B_3(p) \geq p^{2/3} + O(p^{1/3})$.*

The forms used in proving Theorem 3 are all singular $(\operatorname{mod} p)$. It is reasonable to conjecture that $B_3^*(p) \ll p^{1/2+\varepsilon}$, where $B_n^*(p)$ is defined analogously to $B_n(p)$, but with the forms Q restricted to be non-singular $(\operatorname{mod} p)$.

In what follows $\mathbf{x}, \mathbf{y}$, etc. will always be column vectors in $\mathbb{R}^4$ or $\mathbb{Z}^4$ as appropriate. We

Glasgow Math. J. **27** (1985) 87–93.

https://doi.org/10.1017/S0017089500006091 Published online by Cambridge University Press

denote the zero vector by $\mathbf{0}$. We write $\mathbf{x}\,.\,\mathbf{y}$ for the usual scalar product $\mathbf{x}^T\mathbf{y}$. By "$|x_i| \leqslant B$" we shall mean that $|x_i| \leqslant B$ for $1 \leqslant i \leqslant 4$. We will write $\mathbf{x} \pmod p$, as a summation condition, to mean that each component x_i runs from 1 to p. If $p \nmid k$ we write $\bar{k}$ for the inverse of $k \pmod p$. The quadratic form Q will also be thought of as a matrix, also denoted by Q, with entries in the field of p elements. (We will always take $p \geqslant 3$.) With this convention Q^{-1} will be another quadratic form, with coefficients defined $\pmod p$.

2. The Proof of Theorem 3. We shall prove the theorems in reverse order, starting with Theorem 3. Let a be a quadratic non-residue of p and let $b = [p^{1/3}]$. We take

$$Q = (x_1 - bx_2)^2 - a(x_2 - bx_3)^2.$$

Then if $p \mid Q$ we must have $x_1 \equiv bx_2 \pmod p$ and $x_2 \equiv bx_3 \pmod p$. Now if $x_1 \neq bx_2$ we have $|x_1 - bx_2| \geqslant p$, whence

$$(1+b)\mathrm{Max}(|x_1|, |x_2|) \geqslant p.$$

Similarly, if $x_2 \neq bx_3$ then

$$(1+b)\mathrm{Max}(|x_2|, |x_3|) \geqslant p.$$

It follows that

$$\mathop{\mathrm{Max}}_{1 \leqslant i \leqslant 3} |x_i| \geqslant (1+b)^{-1}p = p^{2/3} + O(p^{1/3}),$$

unless $x_1 = bx_2$ and $x_2 = bx_3$. In the latter case a non-zero solution must have $x_3 \neq 0$, whence

$$\mathop{\mathrm{Max}}_{1 \leqslant i \leqslant 3} |x_i| \geqslant |x_1| = b^2|x_3| \geqslant b^2 = p^{2/3} + O(p^{1/3}).$$

This completes the proof of Theorem 3.

3. The Proof of Theorem 2. We begin by showing that, under the conditions of Theorem 2, there are two linear forms $L_1(\mathbf{x}), L_2(\mathbf{x})$ such that $p \mid Q(\mathbf{x})$ whenever $L_1(\mathbf{x}) \equiv L_2(\mathbf{x}) \equiv 0 \pmod p$. To do this we work in the field $\mathbb{F}_p$ of p elements, and look for a form $Q'(x_1', \ldots, x_4')$, equivalent to Q, such that $Q' = 0$ when $x_1' = x_2' = 0$. If Q has rank 2 or less this is immediate, since Q is equivalent to a form $Q'(x_1', x_2')$. If Q has rank 3, then it can be transformed into $Q'(x_1', x_2', x_3')$. By Chevalley's Theorem the latter is a zero form and so is equivalent to $Q''(x_1'', x_2'', x_3'')$ with $Q''(0, 0, 1) = 0$. Hence $Q'' = 0$ if $x_1'' = x_2'' = 0$. Finally, if Q is non-singular then it is equivalent (see for example Borevich and Shafarevich [**1**, Theorem 7, p. 394]) to $Q' = 2x_1'x_2' + Q_0(x_3', x_4')$, since Q is a zero form by Chevalley's Theorem. Here $\det Q_0 = -\det Q$, so that $-\det Q_0$ is a square in $\mathbb{F}_p$. Thus Q_0 factorizes as $Q_0 = 2x_5'x_6'$, whence $Q' = 0$ for $x_1' = x_5' = 0$. The existence of L_1, L_2 now follows in all cases.

The conditions $L_1(\mathbf{x}) \equiv L_2(\mathbf{x}) \equiv 0 \pmod p$ define a sublattice of $\mathbb{Z}^4$ of determinant p^2. It follows from Minkowski's linear forms theorem that there is some non-zero point on the lattice with $\mathrm{Max}\,|x_i| \leqslant p^{1/2}$, and Theorem 2 is proved. (See for example Hardy and Wright [**2**; Theorem 448]. To apply the theorem as it is stated there we note that there is a 4×4 matrix M, of determinant p^2, such that $\boldsymbol{\xi}$ is in the above lattice if and only if $\boldsymbol{\xi} = M\mathbf{x}$ for some $\mathbf{x} \in \mathbb{Z}^4$.)

4. Proof of Theorem 1; preliminaries. We observe at the outset that it suffices to consider the case $n=4$, since in general one may examine the quaternary form obtained from Q by setting $x_5=\ldots=x_n=0$. Moreover, by Theorem 2, we may suppose that $\left(\frac{\det Q}{p}\right)=-1$. Finally, we may take $p\geqslant 3$.

Our key tool is the Poisson summation formula applied to suitable functions $f:\mathbb{R}^4\to\mathbb{R}$. These will have Fourier transform

$$\hat{f}(\mathbf{y})=\int_{\mathbb{R}^4} f(\mathbf{x})e(-\mathbf{x}\,.\,\mathbf{y})\,dx_1\ldots dx_4.$$

Here we have set $e(u)=\exp(2\pi iu)$; we shall also use $e_p(u)$, defined to be $e(u/p)$.

LEMMA 1. *We have*

$$\sum_{\mathbf{x}\in\mathbb{Z}^4,\,p\mid Q(\mathbf{x})} f(\mathbf{x})=p^{-5}\sum_{\mathbf{y}\in\mathbb{Z}^4} S_p(\mathbf{y})\hat{f}\left(\frac{1}{p}\mathbf{y}\right), \tag{3}$$

where

$$S_p(\mathbf{y})=\sum_{s=1}^{p}\sum_{\mathbf{t}(\mathrm{mod}\,p)} e_p(sQ(\mathbf{t})+\mathbf{y}\,.\,\mathbf{t}). \tag{4}$$

Proof. The left hand side of (3) is

$$\frac{1}{p}\sum_{s=1}^{p}\sum_{\mathbf{x}\in\mathbb{Z}^4} e_p(sQ(\mathbf{x}))f(\mathbf{x})=\frac{1}{p}\sum_{s=1}^{p}\sum_{\mathbf{t}(\mathrm{mod}\,p)} e_p(sQ(\mathbf{t}))\sum_{\mathbf{u}\in\mathbb{Z}^4} f(\mathbf{t}+p\mathbf{u}).$$

We apply the Poisson summation formula to $g(\mathbf{u})=f(\mathbf{t}+p\mathbf{u})$. This gives

$$\sum_{\mathbf{u}\in\mathbb{Z}^4} g(\mathbf{u})=\sum_{\mathbf{y}\in\mathbb{Z}^4}\hat{g}(\mathbf{y}),$$

and since

$$\hat{g}(\mathbf{y})=p^{-4}e_p(\mathbf{y}\,.\,\mathbf{t})\hat{f}\left(\frac{1}{p}\mathbf{y}\right)$$

Lemma 1 follows.

LEMMA 2. *Let* $\left(\frac{\det Q}{p}\right)=-1$. *Then*

$$S_p(\mathbf{y})=p^2+p^4Y(\mathbf{y})-p^3Z(\mathbf{y}),$$

where

$$Y(\mathbf{y})=\begin{cases}1, & p\mid\mathbf{y},\\ 0, & p\nmid\mathbf{y},\end{cases}\qquad Z(\mathbf{y})=\begin{cases}1, & p\mid Q^{-1}(\mathbf{y}),\\ 0, & p\nmid Q^{-1}(\mathbf{y}).\end{cases}$$

Proof. We begin by diagonalizing Q. Choose R, invertible (mod p), such that $Q=R^{\mathrm{T}}DR$, with $D=\mathrm{Diag}(d_1,\ldots,d_4)$. We substitute $R\mathbf{t}=\mathbf{u}$ in (4), whence $Q(\mathbf{t})=D(\mathbf{u})$ and

$$\mathbf{y}\,.\,\mathbf{t}=\mathbf{y}^{\mathrm{T}}\mathbf{t}=\mathbf{y}^{\mathrm{T}}R^{-1}\mathbf{u}=\mathbf{v}^{\mathrm{T}}\mathbf{u}=\mathbf{v}\,.\,\mathbf{u}$$

with

$$\mathbf{v} = (R^{-1})^T \mathbf{y}. \tag{5}$$

Thus

$$S_p(\mathbf{y}) = \sum_{s=1}^{p} \sum_{\mathbf{u} \pmod p} e_p(sD(\mathbf{u}) + \mathbf{v} \cdot \mathbf{u})$$
$$= p^4 Y(\mathbf{v}) + \sum_{s=1}^{p-1} \prod_{i=1}^{4} \left\{ \sum_{u_i=1}^{p} e_p(sd_i u_i^2 + v_i u_i) \right\}. \tag{6}$$

Here the term $Y(\mathbf{v})$ is the contribution from $s = p$. From (5) we have $Y(\mathbf{v}) = Y(\mathbf{y})$. Each of the innermost sums in (6) is a standard Gauss sum of the form

$$\sum_{u=1}^{p} e_p(au^2 + bu) = \tau_p \left(\frac{a}{p}\right) e_p(-\overline{4a}b^2), \qquad (p \nmid 4a).$$

Moreover $\tau_p^4 = p^2$ and

$$\prod_{i=1}^{4} \left(\frac{sd_i}{p}\right) = \left(\frac{\det D}{p}\right) = \left(\frac{\det Q}{p}\right) = -1.$$

Thus (6) becomes

$$p^4 Y(\mathbf{y}) - p^2 \sum_{s=1}^{p-1} e_p(-\overline{4s} D^{-1}(\mathbf{v})).$$

Finally we observe that

$$\sum_{s=1}^{p-1} e_p(-\overline{4s}k) = \sum_{t=1}^{p-1} e_p(tk) = \begin{cases} p-1, & p \mid k, \\ -1, & p \nmid k, \end{cases}$$

and that

$$D^{-1}(\mathbf{v}) = \mathbf{v}^T D^{-1} \mathbf{v} = \mathbf{y}^T Q^{-1} \mathbf{y} = Q^{-1}(\mathbf{y}).$$

Lemma 2 now follows.

Lemmas 1 and 2 now yield

$$\sum_{\mathbf{x} \in \mathbb{Z}^4, p \mid Q(\mathbf{x})} f(\mathbf{x}) = p^{-3} \sum_{\mathbf{y} \in \mathbb{Z}^4} \hat{f}\left(\frac{1}{p}\mathbf{y}\right) + p^{-1} \sum_{\mathbf{y} \in \mathbb{Z}^4} \hat{f}(\mathbf{y}) - p^{-2} \sum_{\mathbf{y} \in \mathbf{y}^4, p \mid Q^{-1}(\mathbf{y})} \hat{f}\left(\frac{1}{p}\mathbf{y}\right).$$

We may apply the Poisson summation formula again to the first two sums on the right to produce the following result.

LEMMA 3. *We have*

$$\sum_{\mathbf{x} \in \mathbb{Z}^4, p \mid Q(\mathbf{x})} f(\mathbf{x}) = p^{-1} \sum_{\mathbf{x} \in \mathbb{Z}^4} f(\mathbf{x}) + p \sum_{\mathbf{x} \in \mathbb{Z}^4} f(p\mathbf{x}) - p^{-2} \sum_{\mathbf{y} \in \mathbb{Z}^4, p \mid Q^{-1}(\mathbf{y})} \hat{f}\left(\frac{1}{p}\mathbf{y}\right).$$

Our choice of f will be based on the function considered overleaf.

https://doi.org/10.1017/S0017089500006091 Published online by Cambridge University Press

LEMMA 4. *Define* $g(x)=\begin{cases}1-|x|, & |x|\leqslant 1,\\ 0, & |x|\geqslant 1,\end{cases}$ *so that* $\hat{g}(y)=\left(\frac{\sin \pi y}{\pi y}\right)^2$. *Let* $h(x)=(g*g*g)(x)$. *Then*

(i) $\operatorname{Supp} h\subseteq[-3,3]$,
(ii) $0\leqslant h(x)\leqslant 1$ *for all* x,
(iii) $h(x)\geqslant \frac{1}{32}$ *for* $|x|\leqslant\frac{1}{4}$,
(iv) $\hat{h}(y)=\left(\frac{\sin \pi y}{\pi y}\right)^6$.

Proof. We have

$$h(x)=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} g(u)g(v-u)g(x-v)\,du\,dv. \tag{7}$$

Thus, if $h(x)\neq 0$, there must exist u, v such that $|u|\leqslant 1$, $|v-u|\leqslant 1$, and $|x-v|\leqslant 1$. This requires $|x|\leqslant 3$, proving part (i). The lower bound $h\geqslant 0$ is immediate from (7). Moreover

$$\begin{aligned} h(x)&\leqslant\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} g(u)g(v-u)\,du\,dv\\ &=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} g(u)g(w)\,du\,dw\\ &=\hat{g}(0)^2=1,\end{aligned}$$

which establishes part (ii). For part (iii) we note that if $|u|, |v|, |x|\leqslant\frac{1}{4}$, then $g(u), g(v-u), g(x-v)\geqslant\frac{1}{2}$, while the corresponding area of integration in (7) is $(\frac{1}{2})^2$. Finally (iv) follows from the convolution formula for fourier integrals.

5. Proof of Theorem 1. We begin by applying Lemma 3 with the function

$$f(\mathbf{x})=f_D(\mathbf{x})=\prod_{i=1}^{4} h(x_i/D).$$

From Lemma 4 parts (i) and (ii) we have

$$\begin{aligned}&\sum f_D(\mathbf{x})\leqslant\#\{\mathbf{x}\in\mathbb{Z}^4;|x_i|\leqslant 3D\}\ll D^4,\\ &\sum f_D(p\mathbf{x})\leqslant\#\{\mathbf{x}\in\mathbb{Z}^4;|x_i|\leqslant 3D/p\}=1, \qquad (D<p/3).\end{aligned}$$

By Lemma 4 part (iii) we have $f_D(\mathbf{x})\gg 1$ for $|x_i|\leqslant D/4$, and by part (iv) we have $\hat{f}_D(\mathbf{y})\geqslant 0$. We deduce the following result.

LEMMA 5. *If* $\left(\frac{\det Q}{p}\right)=-1$ *and* $D<p/3$ *then*

$$\#\{\mathbf{x};|x_i|\leqslant D/4, p\mid Q(\mathbf{x})\}\ll p^{-1}D^4+p.$$

Since $Q(\mathbf{x})\equiv 0 \pmod p$ has $O(p^3)$ solutions $(\bmod\, p)$, the lemma is clearly true for $D\geqslant p/3$ too.

https://doi.org/10.1017/S0017089500006091 Published online by Cambridge University Press

We can improve Lemma 5 for small values of D. Suppose that $D \leq \frac{1}{4}p^{1/2}$ and put $P = p^{1/2}(2D)^{-1}$. Consider primes q in the range $P < q \leq 2P$. If $p \mid Q(\mathbf{x})$ with $|x_i| \leq D$, then $p \mid Q(q\mathbf{x})$ and $|qx_i| \leq p^{1/2}$. Hence

$$(\pi(2P)-\pi(P))\#\{\mathbf{x} \neq \mathbf{0};\, |x_i| \leq D,\, p \mid Q(\mathbf{x})\} \leq \sum_{\mathbf{y}} \#\{q;\, P < q \leq 2P,\, q \mid \mathbf{y}\},$$

where $\mathbf{y} \in \mathbb{Z}^4 - \{\mathbf{0}\}$ satisfies $|y_i| \leq p^{1/2}$, $p \mid Q(\mathbf{y})$. However, if $\mathbf{y} \neq \mathbf{0}$ then

$$\#\{q;\, P < q \leq 2P,\, q \mid \mathbf{y}\} \leq \frac{\log p^{1/2}}{\log P}.$$

Moreover $\pi(2P)-\pi(P) \gg \dfrac{P}{\log P}$, whence

$$\begin{aligned}\#\{\mathbf{x} \neq \mathbf{0};\, |x_i| \leq D,\, p \mid Q(\mathbf{x})\} &\ll P^{-1}(\log p)\,.\,\#\{\mathbf{y};\, |y_i| \leq p^{1/2},\, p \mid Q(\mathbf{y})\}\\ &\ll P^{-1}p\,(\log p),\end{aligned}$$

by Lemma 5. On using Lemma 5 itself for $D \geq \frac{1}{4}p^{1/2}$ we now have the following result.

LEMMA 6. *If* $\left(\dfrac{\det Q}{p}\right) = -1$ *then*

$$\#\{\mathbf{x} \in \mathbb{Z}^4;\, |x_i| \leq D,\, p \mid Q(\mathbf{x})\} \ll D^4p^{-1} + Dp^{1/2}(\log p).$$

We apply this not to Q but to Q^{-1}, noting that $\left(\dfrac{\det Q^{-1}}{p}\right) = \left(\dfrac{\det Q}{p}\right) = -1$. We take $f = f_B$, with $p^{1/2} < B < p$, in Lemma 3, whence

$$\begin{aligned}\hat{f}_B\left(\frac{1}{p}\mathbf{y}\right) = B^4 \prod_{i=1}^{4}\left(\frac{\sin \pi y_i B/p}{\pi y_i B/p}\right)^6 &\ll B^4 \prod_{i=1}^{4} \operatorname{Min}\left(1, \left(\frac{p}{B\,|y_i|}\right)^6\right)\\ &\ll B^4 \operatorname{Min}\left(1, \left(\frac{p/B}{\operatorname{Max}|y_i|}\right)^6\right).\end{aligned}$$

We proceed to bound

$$\sum_{\mathbf{y} \in \mathbb{Z}^4,\, p \mid Q^{-1}(\mathbf{y})} \hat{f}\left(\frac{1}{p}\mathbf{y}\right).$$

The term $\mathbf{y} = \mathbf{0}$ contributes $O(B^4)$. We group the remaining terms into ranges $\frac{1}{2}D < \operatorname{Max}|y_i| \leq D$, where D is a power of 2. In such a range there are, by Lemma 6, $\ll D^4p^{-1} + Dp^{1/2}(\log p)$ terms, and each is of magnitude $\ll B^4 \operatorname{Min}\left(1, \left(\dfrac{p}{BD}\right)^6\right)$. The total for $D \leq p/B$ is thus

$$\begin{aligned}\ll B^4 \sum_{D} (D^4p^{-1} + Dp^{1/2}(\log p)) &\ll B^4\left(\left(\frac{p}{B}\right)^4 p^{-1} + \left(\frac{p}{B}\right)p^{1/2}(\log p)\right)\\ &\ll p^3 + p^{3/2}B^3(\log p),\end{aligned}$$

while for $D \geqslant p/B$ it is

$$\ll B^{-2}p^6 \sum_D (D^{-2}p^{-1} + D^{-5}p^{1/2}(\log p))$$

$$\ll B^{-2}p^6\left(\left(\frac{p}{B}\right)^{-2}p^{-1} + \left(\frac{p}{B}\right)^{-5}p^{1/2}(\log p)\right)$$

$$\ll p^3 + p^{3/2}B^3(\log p).$$

Hence

$$p^{-2} \sum_{\mathbf{y}\in\mathbb{Z}^2, p|Q^{-1}(\mathbf{y})} \hat{f}_B\left(\frac{1}{p}\mathbf{y}\right) \ll p^{-2}B^4 + p + p^{-1/2}B^3(\log p) \ll p^{-1/2}B^3(\log p), \tag{8}$$

since $p^{1/2} < B \leqslant p$.

On the other hand $p\sum f_B(p\mathbf{x}) \geqslant 0$ and, by part (iii) of Lemma 4,

$$p^{-1} \sum_{\mathbf{x}\in\mathbb{Z}^4} f_B(\mathbf{x}) \geqslant (32p)^{-1}\#\{\mathbf{x}\in\mathbb{Z}^4;\ |x_i| \leqslant B/4\} \gg p^{-1}B^4. \tag{9}$$

If the implied constants in (8) and (9) are c_1, c_2 respectively, then Lemma 3 yields

$$\sum_{\mathbf{x}\in\mathbb{Z}^4, p|Q(\mathbf{x})} f_B(\mathbf{x}) \geqslant c_2p^{-1}B^4 - c_1p^{-1/2}B^3(\log p) \geqslant \tfrac{1}{2}c_2p^{-1}B^4,$$

providing that $B \geqslant 2c_1c_2^{-1}p^{1/2}(\log p)$. Since the term $\mathbf{x} = \mathbf{0}$ contributes only $1 = o(p^{-1}B^4)$ it follows from Lemma 4 part (i) that $p \mid Q(\mathbf{x})$ with some $\mathbf{x} \neq \mathbf{0}$ for which $|x_i| \leqslant 6c_1c_2^{-1}p^{1/2}(\log p)$. This completes the proof of Theorem 1. Note that it would not have been sufficient to use Lemma 5 in place of Lemma 6.

REFERENCES

1. Z. I. Borevich and I. R. Shafarevich, *Number theory* (Academic Press, New York, 1966).

2. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers* (Oxford University Press, 1960).

3. 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.

MAGDALEN COLLEGE
OXFORD OX1 4AU