COLLOQUIUM MATHEMATICUM

VOL. LXVI 1993 FASC. 2

CUBIC NORMS REPRESENTED BY QUADRATIC SEQUENCES

BY

JACEK POMYKAŁA (WARSZAWA)

1. Introduction. Let $\mathcal{A}$ be a given sequence of positive integers and $\mathcal{K}$ be a Galois extension of the rational numbers of degree l. By $N\mathfrak{a}$ we denote the norm of an integral ideal $\mathfrak{a} \subset \mathcal{K}$. We are interested in whether the equation

$$N\mathfrak{a} = a \tag{1}$$

has arbitrarily many solutions in $\mathfrak{a} \subset \mathcal{K},\ a \in \mathcal{A}$.

For the sequences

$$\mathcal{A} = \{n^2 + 1 : n \text{ a positive integer, } n < x\},$$
$$\mathcal{A} = \{N - N\mathfrak{b} : \mathfrak{b} \subset \mathcal{K}, N\mathfrak{b} < N\}$$

the corresponding problems have been considered in the literature (see [3], [4], [7]).

For the first sequence and $l = 2$ the existence of solutions of (1) was obtained by an application of the $\frac{1}{2}$-dimensional sieve (see [3]). The analogous application of the sieve of dimension $\kappa = 1 - l^{-1}$ with $l = 3$ is not sufficient since the limit of the $\frac{2}{3}$-dimensional sieve is equal to

$$\beta_0 = 1.2242\ldots \tag{2}$$

(see [5]) and it is too large in relation to the value of the distribution level for $\mathcal{A}$.

Therefore the article deals with the more artificial problem

$$N\mathfrak{a} = n^2 + b^2 \quad \text{with } b \text{ prime, } b < n^{\Theta+\varepsilon} \tag{3}$$

(ε an arbitrary positive constant, $0 < \Theta \le 1$).

The smaller Θ, the closer we are to the solution of the original problem. Due to an extra variable b in (3), the resulting distribution level can be greater than x^{β_0}. The crucial point is the application of the new estimates for the exponential sums obtained in [2]. In this direction cf. also [6] and [8].

1991 *Mathematics Subject Classification*: Primary 11L07.

The method presented here works for rather general sequences of the type $\{n^2+b^2 : n \in \mathbb{N},\ n < x,\ b \in \mathcal{B}\}$. However, to avoid the technical difficulties we shall assume that $\mathcal{B}$ is a set of primes. As an application we obtain

THEOREM. *Let $\mathcal{K}$ be a cubic normal extension of the rational numbers and $\mathcal{B}$ be a set of primes such that for $x \to \infty$ we have*

$$\sharp\{b \in \mathcal{B} : b \le x,\ b \equiv 1 \pmod{\lambda}\} \ge x^{\gamma}$$

(γ a constant, $\gamma > 3(\beta_0 - 1)$, λ an integer depending only on $\mathcal{K}$). Then the equation

$$N\mathfrak{a} = n^2 + b^2$$

where $n \in \mathbb{N},\ b \in \mathcal{B},\ n < x,\ b < x^{\Theta+\varepsilon}$ is solvable provided

$$\Theta = \Theta(\gamma, \beta_0) = \frac{6\beta_0 - 7}{2\gamma - 1}\,. \tag{4}$$

As a consequence we deduce for instance that $n^2 + b^2 = N\mathfrak{a}$ for infinitely many pairs (n, b) with b prime, $b < n^{0.35}$.

2. Notation. Technical preparations

- x — a sufficiently large parameter ($x \to \infty$).
- Θ, γ — fixed positive parameters ($0 < \Theta \le 1,\ 0 < \gamma \le 1$).
- $\mathbb{N}$ — the set of positive integers,

$$\mathbb{N}(x) = \{n \in \mathbb{N} : n < x\}\,.$$

- $\mathcal{B}$ — any set of primes greater than λ, with λ a positive integer to be chosen later,

$$\mathcal{B}(x) = \{b \in \mathcal{B} : b < x\}.$$

- $\mathcal{P}$ — any set of primes.
- $\langle d \rangle$ — the integrer part of d.
- $\tau(d)$ — the divisor function, i.e., $\tau(d) = \sum_{d_1 d_2 = d} 1$.
- $\Omega(d)$ — the number of prime divisors of d.
- $\mathbf{e}(t)$ — the additive character $e^{2\pi i t}$.
- $\widehat{f}$ — the Fourier transform of f, i.e., $\widehat{f}(t) = \int_{-\infty}^{\infty} f(\xi)\mathbf{e}(\xi t)\, d\xi$.
- $\ll$ — the Vinogradov symbol, i.e.,

$$f \ll g \Leftrightarrow f = O(g)\,.$$

- (m, n) — the greatest common divisor of m and n.
- $m \equiv a\,(d)$ means $m \equiv a \pmod{d}$.
- $m \sim M$ means $M \le m < 4M$.
- $\|f\|,\ \|f\|_1,\ \|f\|_\infty$ are $L^2,\ L^1,\ L^\infty$ norms of f respectively.

• $S(a,b,c)$ is the Kloosterman sum

$$\sum_{\substack{m\,(\mathrm{mod}\,c)\\(m,c)=1}} \mathbf{e}((am+b\overline{m})/c)$$

where $\overline{m}$ is defined by the congruence condition $m\overline{m}\equiv 1\,(c)$.

• ε — any sufficiently small, positive constant, not necessarily the same at each occurrence.

LEMMA 1. *There exists a function* $\varphi\in C^\infty(\mathbb{R})$ (*with the graph drawn below*) *such that*

$$\varphi(t)=\begin{cases}0 & \textit{for } t\le 0\,,\\ 1 & \textit{for } t\ge 1\,,\end{cases}$$

with derivatives satisfying

$$|\varphi^{(q)}(t)|\le (2^{2q}q!)^2,\qquad q=0,1,2,\dots$$

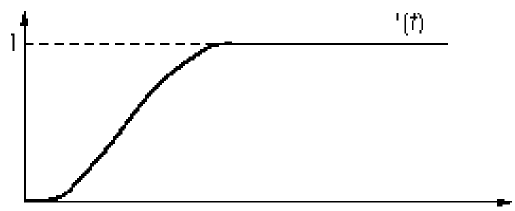

Fig. 1

The proof follows immediately from Lemma 9 of [1]. Using the substitutions $t\to t/2^j$ we obtain

LEMMA 2 (Smooth partitions of unity). *There exists a sequence of functions* $w_j(t)$ *such that*

$$\sum_{j\in\mathbb{Z}} w_j(t)=1\quad \textit{for } t>0,\qquad \operatorname{supp} w_j\subset[2^j,2^{j+2}]\,,$$

$$|w_j^{(q)}(t)|\le (2^{2q}q!)^2\cdot 2^{-jq},\qquad q=0,1,2,\dots$$

LEMMA 3 (Truncated Poisson formula for arithmetic progressions). *Let* f *be a smooth function with compact support in* $[y,4y]$, *where* $y>0$, *such that*

$$f^{(q)}(t)\ll y^{-q},\qquad q=0,1,2,\dots,$$

with the constant implied in the symbol $\ll$ *depending on* q *only. Then*

$$\sum_{m\equiv a\,(d)} f(m)=d^{-1}\sum_{|h|\le d^{1+\varepsilon}y^{-1}} \widehat{f}(h/d)\mathbf{e}(-ah/d)+O(d^{-1})\,.$$

The proof follows immediately by integration by parts $\langle 2/\varepsilon\rangle+2$ times.

We define the sequence

$$\mathcal{A} = \{(\lambda n)^2 + b^2 : \ n \in \mathbb{N}(x), \ b \in \mathcal{B}(x^{\Theta}), \ (\lambda n, b) = 1\}.$$

For technical reasons we introduce smooth functions drawn below with derivatives satisfying

$$g^{(q)}(t) \ll t^{-q}, \quad B^{(q)}(t) \ll t^{-q}, \quad q = 0, 1, 2, \ldots$$

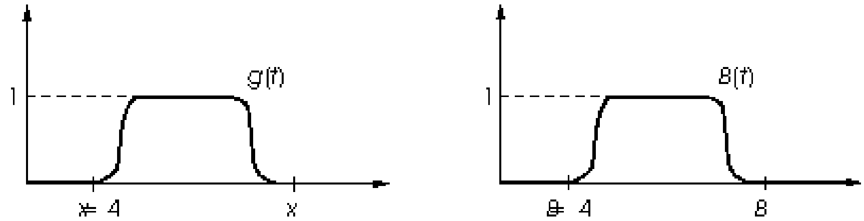

Fig. 2

Here $B = x^{\Theta}$.

In the sequel we shall use the abbreviated notation $|\mathcal{B}|$ for the number of elements in the set $\mathcal{B}(B)$.

For a given $\mathcal{P}$ and $z \geq 2$ define

$$P(z) = \prod_{p \in \mathcal{P}, p < z} p.$$

We define the sifting function (modified by the weight functions $g(t), B(t)$) as follows:

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, z) = \sum_{\substack{(\lambda n, b) = 1 \\ ((\lambda n)^2 + b^2, P(z)) = 1}} B(b) g(n)$$

where the double summation is taken over $b \in \mathcal{B}$ and $n \in \mathbb{N}$.

Next we shall need some results of algebraic character.

Lemma 4 (see [4]). *There exists a Δ divisible by all ramified primes, and only by them, such that a prime p splits completely in $\mathcal{K}$ if and only if*

$$p \pmod{\Delta} \in \mathcal{H}$$

where $\mathcal{H}$ is the subgroup of index 3 *in the group $\mathbb{Z}_{\Delta}^*$ of residue classes modulo Δ, coprime with Δ.*

By Lemma 4 it follows that if a positive integer m satisfies

$$p \mid m \Rightarrow p \pmod{\Delta} \in \mathcal{H}$$

then m is represented by the norm of an ideal $\mathfrak{a} \subset \mathcal{K}$. We take as $\mathcal{B}$ the set of primes congruent to $1 \pmod{4\Delta}$. Letting ϕ be the natural homomorphism

$$\phi : \mathbb{Z}_{4\Delta}^* \to \mathbb{Z}_{\Delta}^* \quad (\phi : a \pmod{4\Delta} \to a \pmod{\Delta}))$$

we set $\mathcal{H}' = \phi^{-1}(\mathcal{H})$. Then we have

LEMMA 5. *Let $\mathcal{G}$ be the subgroup of $\mathbb{Z}^*_{4\Delta}$ defined by*

$$\mathcal{G} = \{g \in \mathbb{Z}^*_{4\Delta} : g \equiv 1\,(4)\}\,.$$

Then $(\mathcal{H}' : \mathcal{H}' \cap G) = 2$.

Proof. The natural epimorphism $\phi_1 : \mathbb{Z}^*_{4\Delta} \to \mathbb{Z}^*_4$ maps $\mathcal{H}'$ onto $\mathbb{Z}^*_4$ since otherwise $\mathcal{H}' = \phi_1^{-1}(1)$ would have an even index in $\mathbb{Z}^*_{4\Delta}$, which contradicts the assumption $(\mathbb{Z}^*_{4\Delta} : \mathcal{H}') = 3$. Therefore $(\mathcal{H}' : \mathcal{H}' \cap \mathcal{G}) = |\mathcal{H}'/\mathcal{H}' \cap \ker\phi_1| = 2$ as required.

3. The sieving problem and the estimate of the main term. We start this section by the remark that the proof of the Theorem reduces to the nontrivial lower bound for the sifting function $S(\mathcal{A}, \mathcal{P}, z)$, where

$$\mathcal{P} = \{p \text{ prime} : (p, \lambda) = 1,\ p \pmod{\lambda} \notin \mathcal{H}'\}\,,$$
$$z = (\lambda + 1)x, \qquad \lambda = 4\Delta\,.$$

Let $a \in \mathcal{A}$. We observe that if a prime p such that $p \,|\, a$ is in $\mathcal{H}'$ then by Lemma 4 it is of the form $N\mathfrak{a}$ for some $\mathfrak{a} \subset \mathcal{K}$.

Since $\mathcal{H}'$ is a subgroup of $\mathbb{Z}^*_\lambda$ we see from the congruence condition

$$a = (\lambda n)^2 + b^2 \equiv 1 \pmod{\lambda}$$

that $a \in \mathcal{H}'$. Moreover, the group structure of $\mathcal{H}'$ ensures that $a = (\lambda n)^2 + b^2$ cannot have exactly one prime factor outside $\mathcal{H}'$. Therefore it is sufficient to sift the sequence $\mathcal{A}$ by the primes $p \notin \mathcal{H}$ not exceeding the value $(\lambda^2 x^2 + x^2)^{1/2} < (\lambda + 1)x$.

To complete the proof of the Theorem it remains to estimate (from below) the sifting function $S(\mathcal{A}, \mathcal{P}, z)$. We shall use the results obtained in [5].

Let $D > 1$. By $\mu_d^- = \mu_d^-(D)$ we denote the Rosser weights of the lower $\frac{2}{3}$-dimensional sieve ($|\mu_d^-| \le 1$). In view of Lemma 1 of [5] we have

$$\begin{aligned}
\mathcal{S}(\mathcal{A}, \mathcal{P}, z) &= \sum_{(\lambda n, b) = 1} \sum B(b) g(n) \sum_{\substack{d | (\lambda n)^2 + b^2 \\ d | P(z)}} \mu(d) \\
&\ge \sum_{(\lambda n, b) = 1} \sum B(b) g(n) \sum_{\substack{d | (\lambda n)^2 + b^2 \\ d | P(z)}} \mu_d^- \\
&= \sum_{d | P(z)} \mu_d^- \sum_{\substack{(\lambda n, b) = 1 \\ (\lambda n)^2 + b^2 \equiv 0\,(d)}} B(b) g(n) = \sum_{d | P(z)} \mu_d^- |\mathcal{A}_d|
\end{aligned}$$

where $\mu(d)$ is the Möbius function and

$$\begin{aligned}|\mathcal{A}_d| &= \sum_{(b,\lambda d)=1} B(b) \sum_{\substack{(n,b)=1\\(\lambda n)^2+b^2\equiv 0\,(d)}} g(n)\\ &= \sum_{(b,d)=1} B(b)\Big\{\sum_{\substack{n\in\mathbb{N}\\(\lambda n)^2+b^2\equiv 0\,(d)}} g(n) - \sum_{\substack{n\equiv 0\,(b)\\(\lambda n)^2+b^2\equiv 0\,(d)}} g(n)\Big\}\\ &= \sum_{(b,d)=1} B(b) \sum_{\vartheta\,(\mathrm{mod}\,d)} \Big\{\sum_{n\equiv\vartheta b\,(d)} g(n) - \sum_{n\equiv\vartheta\,(d)} g(nb)\Big\}.\end{aligned}$$

Here ϑ (mod d) runs over the solutions of the congruence $\lambda^2t^2+1\equiv 0\,(d)$. Letting $\varrho(d)$ stand for the number of such solutions we obtain, by Lemma 3,

$$\begin{aligned}|\mathcal{A}_d| &= \sum_{(b,d)=1} B(b) \sum_{\vartheta\,(\mathrm{mod}\,d)} d^{-1}\Big\{\sum_{|h|<d^{1+\varepsilon}/x} \widehat{g}\Big(\frac{h}{d}\Big)\mathbf{e}\Big(-\vartheta b\frac{h}{d}\Big)\\ &\quad + \sum_{|h|<d^{1+\varepsilon}B/x} b^{-1}\widehat{g}\Big(\frac{h}{bd}\Big)\mathbf{e}\Big(-\vartheta\frac{h}{d}\Big)\Big\} + O(|\mathcal{B}|\varrho(d)d^{-1})\\ &= \frac{\varrho(d)}{d}\widehat{g}(0)\sum_{b\in\mathcal{B}} B(b)\Big(1+\frac{1}{b}\Big) + r'(\mathcal{A},d)\\ &= \frac{\varrho(d)}{d}\widehat{g}(0)\sum_{b\in\mathcal{B}} B(b) + r(\mathcal{A},d)\end{aligned}$$

where

$$r(\mathcal{A},d) = r_1(\mathcal{A},d)+r_2(\mathcal{A},d) + O\Big(\frac{\varrho(d)}{d}\Big(\widehat{g}(0)\sum_{(b,d)>1}(1+B(b))+|\mathcal{B}|\Big)\Big), \tag{5}$$

$$\begin{aligned}r_1(\mathcal{A},d) &= \sum_{(b,d)=1}\sum_{\vartheta} d^{-1}\sum_{\substack{h\neq 0\\ h<d^{1+\varepsilon}/x}} \widehat{g}\Big(\frac{h}{d}\Big)\mathbf{e}\Big(-\vartheta b\frac{h}{d}\Big),\\ r_2(\mathcal{A},d) &= \sum_{(b,d)=1}\sum_{\vartheta}(bd)^{-1}\sum_{\substack{h\neq 0\\ h<Bd^{1+\varepsilon}/x}} \widehat{g}\Big(\frac{h}{bd}\Big)\mathbf{e}\Big(\vartheta\frac{h}{d}\Big).\end{aligned} \tag{6}$$

Therefore

$$\begin{aligned}\mathcal{S}(\mathcal{A},\mathcal{P},z) \ge \sum_{d|P(z)}\mu_d^-|\mathcal{A}_d| &= \widehat{g}(0)\sum_{b\in\mathcal{B}} B(b)\sum_{d|P(z)}\mu_d^-\frac{\varrho(d)}{d} + \sum_{d|P(z)}\mu_d^- r(\mathcal{A},d)\\ &= \text{main term} + \text{remainder term}.\end{aligned}$$

In the next section we shall prove the following estimate for the remainder term:

$$\sum_{d<D} |r(\mathcal{A}, d)| \le |\mathcal{B}| x^{1-\varepsilon} \tag{7}$$

provided $D = x^{\alpha_0 - 19\varepsilon}$, where

$$\alpha_0 = \alpha_0(\gamma, \Theta) = \min\left\{1 + \gamma\Theta, \frac{4}{3} - \frac{\Theta(1-\gamma)}{3}, \frac{7}{6} + \frac{\Theta}{6}(2\gamma - 1)\right\}. \tag{7'}$$

Obviously, if Θ is defined by (4) and $\gamma > 3(\beta_0 - 1)$ then

$$\alpha_0(\gamma, \Theta) = \beta_0 .$$

The main term will be evaluated by means of the following result (see [5]).

Lemma 6. *Let $\omega(d)$ be any multiplicative function satisfying*

(i) $0 \le \omega(p) < p$ *for* $p \in \mathcal{P}$,

(ii) *there exists a constant* $C \ge 2$ *such that for all* $z > w \ge 2$,

$$\prod_{p \in \mathcal{P}, w \le p < z} (1 - \omega(p)/p)^{-1} \le \left(\frac{\log z}{\log w}\right)^{2/3} \left\{1 + \frac{C}{\log w}\right\}.$$

Then

$$\sum_{d | P(z)} \omega(d) d^{-1} \mu_d^-(D) \ge \prod_{p | P(z)} (1 - \omega(p)/p)\{f(s) + O[e^{\sqrt{C} - s}(\log D)^{-1/3}]\}$$

where $s = \log D / \log z$ *and* $f(s)$ *is positive provided* $s > \beta_0$.

To complete the proof of the Theorem we notice that for

$$\omega(p) = \varrho(p) = \begin{cases} 2 & \text{if } p \in \mathcal{P},\ p \equiv 1\,(4)\,, \\ 0 & \text{if } p \in \mathcal{P},\ p \equiv 3\,(4)\,, \end{cases}$$

the Mertens prime number theory and Lemmas 4 and 5 imply the inequality

$$\prod_{\substack{p \in \mathcal{P} \\ w \le p < z}} (1 - \varrho(p) p^{-1})^{-1} \le \left(\frac{\log z}{\log w}\right)^{2/3} \left\{1 + \frac{C}{\log w}\right\}$$

with some constant $C = C(\lambda)$. Hence by Lemma 6 with $\omega(d) = \varrho(d)$, (7) and (7′) we conclude that $\mathcal{S}(\mathcal{A}, \mathcal{P}, z)$ is positive provided $\alpha_0(\gamma, \Theta) > \beta_0$. This completes the proof of the Theorem.

4. Estimate of the remainder term. Applying the smooth partitions of unity $\{w_{j_1}(h)\}_{j_1 \in \mathbb{Z}}$, $\{w_{j_2}(d)\}_{j_2 \in \mathbb{Z}}$ in the right-hand side of (6) we conclude that the estimate (7) reduces to

$$(8)\quad \sum_{d\sim D}\sum_{\vartheta\,(\mathrm{mod}\,d)}\Big|\sum_{\substack{b\in\mathcal{B}\\(b,d)=1}}\sum_{h\sim H} w_{j_1}(h)w_{j_2}(d)B(b)\widehat{g}^{(e)}\Big(\frac{h}{d}\Big)\mathbf{e}\Big(-hb^{1-e}\frac{\vartheta}{d}\Big)\Big| + (x+|\mathcal{B}|)\sum_{d<D}\varrho(d)\Omega(d) \ll |\mathcal{B}|Dx^{1-2\varepsilon},$$

where

$$H\le Dx^{-1}B^e x^{\varepsilon/2},\qquad \widehat{g}^{(e)}\Big(\frac{h}{d}\Big) = \int g(b^e\eta)\mathbf{e}\Big(\eta\frac{h}{d}\Big)d\eta,$$
$$e=0 \text{ or } 1 \quad\text{and}\quad D=x^{\alpha_0-19\varepsilon}.$$

Moreover, the condition $(b,d)=1$ in the first term of (8), and the second term in (8), may be omitted, since for $(b,d)>1$ the suitable contribution to the left-hand side of (8) is bounded by

$$\ll DH\widehat{g}^{(e)}(0)x^{\varepsilon}\le D^2x^{2\varepsilon}\le|\mathcal{B}|Dx^{1-2\varepsilon}$$

(since $\alpha_0\le 1+\gamma\Theta$ by (7′)), while the second term contributes $Dx^{1+\varepsilon}$, which is $\ll|\mathcal{B}|Dx^{1-2\varepsilon}$ since $\gamma\Theta>0$.

Now the application of Cauchy's inequality reduces our problem to the proof of the inequality

$$\sum_{b_1,b_2\in\mathcal{B}}\sum_{h_1,h_2\sim H}\sum_{d\sim D}\sum_{\vartheta\ (\mathrm{mod}\ d)} w_{j_1}(h)\mathbf{e}\Big((h_1b_1^{1-e}-h_2b_2^{1-e})\frac{\vartheta}{d}\Big)G(d,b_1,b_2,h_1,h_2) \ll D|\mathcal{B}|^2B^{2e}x^{-5\varepsilon}$$

where

$$G(d,b_1,b_2,h_1,h_2) = w_{j_1}(h_1)w_{j_1}(h_2)w_{j_2}(d)B(b_1)B(b_2)\mathbf{e}\Big((h_1-h_2)\frac{\eta}{d}\Big)g(b_1^e\eta)g(b_2^e\eta).$$

Let $k=h_1b_1^{1-e}-h_2b_2^{1-e}$. The diagonal $k=0$ provides an admissible contribution since

- if $e=0$ it is
$$\ll Dx^{\varepsilon}\sum_{b_1,h_1}1\ll D|\mathcal{B}|Hx^{\varepsilon}\ll D^{2+\varepsilon}|\mathcal{B}|x^{-1+\varepsilon}B^e\ll D|\mathcal{B}|^2B^{2e}x^{-5\varepsilon},$$
- if $e=1$ it is
$$\ll D|\mathcal{B}|^2Hx^{\varepsilon}\ll|\mathcal{B}|^2D^2x^{\varepsilon-1}B\ll|\mathcal{B}|^2DB^2x^{-5\varepsilon}$$

(in view of the condition $\alpha_0\le 1+\Theta$, see (7′)).

Now we consider $k \sim K$ with $1 \le K \le HB^{1-e} \le D^{1+\varepsilon}x^{-1}B$ and investigate the exponential sum

$$T_e(x,\mathcal{B},D) = \sum_{(k)} \sum_{d\sim D} \sum_{\vartheta \,(\mathrm{mod}\, d)} \mathbf{e}\Big(k\frac{\vartheta}{d}\Big) G(d,b_1,b_2,h_1,h_2)$$

where $\sum_{(k)}$ denotes the summation over the variables b_1, b_2, h_1, h_2 such that $h_1 b_1^{1-e} - h_2 b_2^{1-e} \sim K$. Our aim is to show that

$$T_e(x,\mathcal{B},D) \ll D|\mathcal{B}|^2 B^{2e} x^{-6\varepsilon} \tag{9}$$

provided $D = x^{\alpha_0 - 19\varepsilon}$.

4.1. *Application of Gaussian theory of binary quadratic forms.* The following result can be inferred from the article 86 of [9].

LEMMA 7 (see [3]). *Let $f(y) = ay^2 + by + c$ be a polynomial with integer coefficients ($a > 0$) and discriminant $\partial = b^2 - 4ac < -4$. Select one form (α,β,γ) from each class of primitive definite forms of determinant ∂ ([1]). There exists a one-to-one correspondence between the roots of*

$$f(\vartheta) \equiv 0 \pmod d$$

and the pairs $\pm(r,s)$ of proper representations of $4ad$ by the given forms, such that

$$\alpha r + (\beta + b)s \equiv 0\,(2a). \tag{10}$$

This correspondence is given by

$$\frac{\vartheta}{d} = 2\Big(\frac{\overline{r}}{s} - \frac{\alpha r + (\beta+b)s}{s(\alpha r^2 + 2\beta rs + \gamma s^2)}\Big) \tag{11}$$

where

$$r\overline{r} \equiv 1\,(s)\,.$$

Remark. Since we may choose the forms (α,β,γ) satisfying $(\alpha\beta, 2a) = 1$, the conditions $(r,s) = 1$ and $\alpha r + 2\beta rs + \gamma s^2 = 4ad$ imply that $(s,2a) = 1$, hence $s \neq 0$ and thus the right-hand side of (11) is well defined.

We apply Lemma 7 to

$$\partial = -4\lambda^2, \quad a = \lambda^2, \quad b = 0, \quad c = 1\,.$$

Denoting by $\mathcal{F} = \mathcal{F}(\partial)$ the system of representing forms $\psi = (\alpha,\beta,\gamma)$ we have

(12) $T_e(x,\mathcal{B},D)$

$$= \frac{1}{2} \sum_{\psi\in\mathcal{F}} \sum_{(k)} \sum_{\substack{(r,s)=1 \\ \alpha r + \beta s \equiv 0\,(2\lambda^2)}} \mathbf{e}\Big(2k\frac{\overline{r}}{s}\Big) G\Big(\frac{\psi(r,s)}{4\lambda^2}, b_1, b_2, h_1, h_2\Big) \mathbf{e}\Big(-2k\frac{\alpha r + \beta s}{s\psi(r,s)}\Big).$$

([1]) Following Gauss' notation we denote by (α,β,γ) the form with coefficients $\alpha, 2\beta, \gamma$.

Since $(\alpha\beta, 2\lambda) = 1$ we may split the summation over r, s above into a double sum over s such that $(s, 2\lambda) = 1$ and over r coprime with s such that $r \equiv -\beta\overline{\alpha}s\,(2\lambda^2)$, with $\alpha\overline{\alpha} \equiv 1\,(2\lambda^2)$. Moreover, applying the smooth partitions of unity $\{w_{j_3}(r)\}_{j_3\in\mathbb{Z}}$, $\{w_{j_4}(s)\}_{j_4\in\mathbb{Z}}$ we obtain

$$T_e(x, \mathcal{B}, D) \ll x^{\varepsilon} \max_{R,S} \sum_{(k)} \sum_{\substack{(s,2\lambda)=1 \\ s\sim S}} \sum_{\substack{r\sim R,(r,s)=1 \\ r\equiv -\beta\bar{\alpha}s\,(2\lambda^2)}} \mathbf{e}\left(2k\frac{\overline{r}}{s}\right) G_1(r)$$

where $\overline{\alpha}, \beta$ are fixed numbers that depend only on λ and the maximum is taken over

$$1 \le R, S \le C_\lambda D^{1/2}\,,$$

with some constant C_λ depending only on λ. The function $G_1(r)$ has the form

$$G_1(r) = G\left(\frac{\psi(r,s)}{4\lambda^2}, b_1, b_2, h_1, h_2\right)\mathbf{e}\left(-2k\frac{\alpha r + \beta s}{s\psi(r,s)}\right) w_{j_3}(r) w_{j_4}(s)\,.$$

By Lemma 3 the innermost sum over $r \sim R$ in the right-hand side of (12) is equal to

$$(13)\qquad \sum_{r\equiv\beta\bar{\alpha}s\,(2\lambda^2)} G_1(r)\mathbf{e}\left(2k\frac{\overline{r}}{s}\right) r$$

$$= \sum_{\substack{\nu \pmod s \\ (\nu,s)=1}} \mathbf{e}\left(2k\frac{\overline{\nu}}{s}\right) \sum_{\substack{r\equiv\nu\,(s) \\ r\equiv\beta\alpha s\,(2\lambda^2)}} G_1(r)$$

$$= \sum_{\substack{\nu \pmod s \\ (\nu,s)=1}} \mathbf{e}\left(2k\frac{\overline{\nu}}{s}\right)(2\lambda^2 s)^{-1}$$

$$\times \left(\sum_{|m|\le S^{1+\varepsilon}/R} \mathbf{e}\left(-\frac{m}{2\lambda^2 s}(2\lambda^2\nu\overline{2\lambda^2} - \beta\overline{\alpha}s)\right)\widehat{G}_1\left(\frac{m}{2\lambda^2 s}\right) + O(1)\right)$$

$$= \sum_{|m|\le S^{1+\varepsilon}/R} \mathbf{e}\left(-\frac{\beta\overline{\alpha}}{2\lambda^2}m\right)$$

$$\times \sum_{\substack{\nu \pmod s \\ (\nu,s)=1}} \mathbf{e}\left(\frac{\overline{\nu}2k - \nu\overline{2\lambda^2}m}{s}\right)\widehat{G}_1\left(\frac{m}{2\lambda^2 s}\right)(2\lambda^2 s)^{-1} + O(1)$$

$$= \sum_{|m|\le S^{1+\varepsilon}/R} \mathbf{e}\left(-\frac{\beta\overline{\alpha}}{2\lambda^2}m\right) S(2k, -\overline{2\lambda^2}m, s)\widehat{G}_1\left(\frac{m}{2\lambda^2 s}\right)(2\lambda^2 s)^{-1} + O(1)\,.$$

Here $S(k,\overline{-2\lambda^2}m,s)$ is the Kloosterman sum. The error $O(1)$ contributes to $T_e(x,\mathcal{B},D)$ a quantity less than

$$x^\varepsilon \max_{R,S}\sum_{(k)}\sum_{s\sim S} 1 \ll x^{2\varepsilon}H^2|\mathcal{B}|^2\mathcal{S} \ll x^{4\varepsilon}D^{5/2}x^{-2}B^{2e}|\mathcal{B}|^2$$
$$\ll D|\mathcal{B}|^2B^{2e}x^{-6\varepsilon}, \quad \text{since } D\le x^{4/3} \text{ by } (7')\,.$$

In view of (9) this proves that the above error is admissible. In the case $m=0$ the Kloosterman sum reduces to a Ramanujan sum, hence by the well known estimate we find that the corresponding contribution to $T_e(x,\mathcal{B},D)$ does not exceed

$$\max_{R,S}\sum_{(k)}\sum_{s\sim S} S(2k,0,s)RS^{-1}x^\varepsilon \ll x^{2\varepsilon}D^{1/2}H^2|\mathcal{B}|^2 \ll D|\mathcal{B}|^2B^{2e}x^{-6\varepsilon}$$

as above. Therefore we shall assume in the sequel that $m\neq 0$, which implies that $S^{1+\varepsilon}\ge R$. In view of Lemma 7 we have $(S^{1+\varepsilon})^2+S^2\gg D$, hence $D^{1/2-\varepsilon}\le S\le C_\lambda D^{1/2}$. Applying the smooth partition of unity $\{w_{j_5}(m)\}_{j_5\in\mathbb{Z}}$ we have, by (12) and (13),

$$T_e(x,\mathcal{B},D)\ll x^{8\varepsilon}\max_{H,K,S,M}E(H,K,S,M) + \text{admissible error term} \tag{14}$$

where

$$\begin{aligned} E(H,K,S,M) = R\sum_{(k)}\sum_{m\sim M}&\mathbf{e}\Big(\frac{-\beta\overline{\alpha}}{2\lambda^2}m\Big)\\ &\times\sum_{(s,2\lambda)=1} s^{-1}S(2k,\overline{-2\lambda^2}m,s)G_2(m,b_1,b_2,h_1,h_2,s)\end{aligned} \tag{15}$$

and the maximum is taken over

$$\begin{aligned} &1\le H\le Dx^{-1}B^e x^{\varepsilon/2}\,,\\ &1\le K\le HB^{1-e}\le DBx^{-1+\varepsilon/2}\,,\\ &D^{1/2-\varepsilon}\le S\le C_\lambda D^{1/2}\,,\\ &1\le M\le SR^{-1}x^\varepsilon, \quad R\le Sx^\varepsilon\,.\end{aligned} \tag{16}$$

Here G_2 is defined as follows:

$$\begin{aligned} G_2(m,&b_1,b_2,h_1,h_2,s)\\ &= G\Big(\frac{\psi(\xi,s)}{4\lambda^2},b_1,b_2,h_1,h_2\Big)\\ &\quad\times\mathbf{e}\Big(-2k\frac{\alpha\xi+\beta s}{s\psi(\xi,s)}\Big)\mathbf{e}\Big(\frac{m\xi}{2\lambda^2 s}\Big)w_{j_3}(\xi)w_{j_4}(s)w_{j_5}(m)x^{-6\varepsilon}\end{aligned}$$

where ξ is a fixed parameter ($R\le\xi\le 4R$).

Letting $\underline{x} = (x_1, \ldots, x_5) \in \mathbb{R}^5$ we see by the definition of G that

$$\frac{\partial^{q_1+\ldots+q_5}}{\partial x_1^{q_1} \cdots \partial x_5^{q_5}} G_2(\underline{x}, s) \ll \prod_{j=1}^{5} x_j^{-q_j} \qquad (0 \le q_j \le 2,\ j = 1, \ldots, 5)\,. \tag{17}$$

For the s-derivatives, one obtains

$$\begin{aligned} \frac{\partial^\nu}{\partial s^\nu} G_2(\underline{x}, s) &\ll s^{-\nu}(1 + KD^{-1})^\nu x^{-2\varepsilon} \\ &\ll s^{-\nu}\,, \qquad \nu = 0, 1, 2 \text{ (since } \Theta \le 1)\,. \end{aligned} \tag{18}$$

4.2. *Estimate for sum of Kloosterman sums.* In this section we apply the method developed by Deshouillers and Iwaniec in [2] for the group $\Gamma = \Gamma_0(v)$, with $v = 2\lambda^2$. We start from the separation of variables in $G_2(\overline{x}, s)$. Let

$$u = \frac{4\pi\sqrt{x_1 k}}{s\sqrt{v}}$$

where

$$k = k(\underline{x}) = x_4 x_2^{1-e} - x_5 x_3^{1-e}\,.$$

Then

$$G_2(\underline{x}, s) = \int_{\mathbb{R}^5} \psi_{\underline{t}}(u) \mathbf{e}(\underline{t}\ \underline{x})\, d\underline{t} \tag{19}$$

where $\underline{t} = (t_1, \ldots, t_5)$ and by the inversion formula

$$\psi_{\underline{t}}(u) = \int_{\mathbb{R}^5} G_2\left(\underline{x}, \frac{4\pi\sqrt{x_1 k}}{u\sqrt{v}}\right) \mathbf{e}(-\underline{x}\ \underline{t})\, d\underline{x}\,.$$

For $t_1, \ldots, t_5 \ne 0$ integrating by parts q_j times with respect to x_j ($j = 1, \ldots, 5$) and then differentiating ν times with respect to u we obtain, by (17) and (18),

$$\begin{aligned} \frac{\partial^\nu}{\partial u^\nu} \psi_{\underline{t}}(u) &= \prod_{j=1}^{5} (2\pi t_j)^{-q_j} \\ &\quad \times \int_{\mathbb{R}^5} \frac{\partial^{q_1+\ldots+q_5+\nu}}{\partial x_1^{q_1} \ldots \partial x_5^{q_5} \partial u^\nu} G_2\left(\underline{x}, \frac{4\pi\sqrt{x_1 k}}{u\sqrt{v}}\right) \mathbf{e}(-\underline{x}\ \underline{t})\, d\underline{x} \\ &\ll (t_1 M)^{-q_1} (t_2 B)^{-q_2} (t_3 B)^{-q_3} (t_4 H)^{-q_4} (t_5 H)^{-q_5} (\sqrt{MK}/S)^{-\nu} M B^2 H^2 \end{aligned} \tag{20}$$

where $0 \le q_j \le 2,\ 0 \le \nu \le 2,\ j = 1, \ldots, 5$.

In view of (15) and (19) we have

$$E(H, K, S, M) = R \sum_{(k)} \sum_{m \sim M} \mathbf{e}\left(\frac{\beta\overline{\alpha}}{2\lambda^2} m\right) \sum_{\substack{(s, 2\lambda)=1 \\ s \sim S}} s^{-1} S(2k, \overline{2\lambda^2} m, s) \tag{21}$$

$$\times \int\limits_{\mathbb{R}\setminus\{0\}} \dots \int\limits_{\mathbb{R}\setminus\{0\}} \psi_{\underline{t}}(u)\mathbf{e}(t_1 m)\mathbf{e}(t_2 b_1)\mathbf{e}(t_3 b_2)\mathbf{e}(t_4 h_1)\mathbf{e}(t_5 h_2)\, dt_1 \dots dt_5$$

since the remaining set of integration has measure 0 in $\mathbb{R}^5$.

For any $\underline{t} \neq \underline{0}$ the function $\psi_{\underline{t}}(u)$ satisfies

$$\operatorname{supp} \psi_{\underline{t}} \subset [X,\, 16X] \quad \text{with} \quad X = \frac{\pi\sqrt{MK}}{S\sqrt{v}}\,,$$

$$\psi_{\underline{t}}(u) \ll (t_1 M)^{-q_1} (T_2 B)^{-q_2} (t_3 B)^{-q_3} (t_4 H)^{-q_4} (t_5 H)^{-q_5} M B^2 H^2\,.$$

Therefore there exists $\delta > 0$ such that the function

$$\Phi_{\underline{t}}(u) = \delta (t_1 M)^{q_1} (t_2 P)^{q_2} (t_3 P)^{q_3} (t_4 H)^{q_4} (t_5 H)^{q_5} (M B^2 H^2)^{-1} \psi_{\underline{t}}(u)$$

satisfies

$$\operatorname{supp} \Phi_{\underline{t}} \subset [X,\, 16X], \qquad \|\Phi_{\underline{t}}\|_\infty \le 1\,,$$

$$\|\Phi'_{\underline{t}}\|_1 = \int\limits_X^{16X} \left|\frac{\partial}{\partial u}\Phi_{\underline{t}}(u)\right| du \le \frac{\sqrt{v}}{16\pi} \int\limits_X^{16X} \left(\frac{\sqrt{MK}}{S}\right)^{-1} du \le 1\,,$$

$$\|\Phi''_{\underline{t}}\| = \int\limits_X^{16X} \left|\frac{\partial^2}{\partial u^2}\Phi_{\underline{t}}(u)\right| du \le \frac{v}{16\pi^2} \int\limits_X^{16X} \left(\frac{\sqrt{MK}}{S}\right)^{-2} du \le X^{-1}\,.$$

The required bound for $E(H,K,S,M)$ is due to the following

LEMMA 8. *Let $\Phi(u)$ be a smooth function satisfying*

$$\operatorname{supp} \Phi \subset [X, 16X]\,,$$

$$\|\Phi\|_\infty \le 1, \quad \|\Phi'\|_1 \le 1, \quad \|\Phi''\|_1 \le X^{-1}\,.$$

Then

$$\sum_{\substack{(s,v)=1 \\ s\sim S}} s^{-1} \sum_{k\sim K} b_k \sum_{m\sim M} a_m S(2k, \overline{v}m, s) \Phi\biggl(\frac{4\pi\sqrt{mk}}{s\sqrt{v}}\biggr) \tag{22}$$

$$\ll \biggl[1 + \frac{1+X^{-1/2}}{1+X}(1+X+\sqrt{M})(1+X+\sqrt{K})\|a_m\|\,\|b_k\|\biggr](MKS)^\varepsilon\,.$$

Proof. Follows from [2], Theorem 8, p. 234, by the observation that $0 \le \Theta_q \le 1/2$, $\mu(\mathfrak{a}) \ll 1$, $\mu(\mathfrak{b}) \ll 1$.

In view of (21) and (22) we have

$$E(H,K,S,M)$$

$$\ll R \int\limits_{\mathbb{R}\setminus\{0\}} \dots \int\limits_{\mathbb{R}\setminus\{0\}} \biggl[1 + \frac{1+X^{-1/2}}{1+X}(1+X+\sqrt{M})(1+X+\sqrt{K})\|a_m\|\,\|b_k\|\biggr]$$

$$\times (MKS)^\varepsilon M B^2 H^2 (t_1 M)^{-q_1} \dots (t_5 H)^{-q_5}\, dt_1 \dots dt_5$$

where

$$\|a_m\|^2 = \sum_{m\sim M}\left|\mathbf{e}\left(\frac{-\beta\overline{\alpha}}{v}m\right)\mathbf{e}(t_1m)\right|^2 \le 4M\,,$$

$$\begin{aligned}\|b_k\|^2 &= \sum_{k\sim K}\Big|\sum_{\substack{h_1,b_1,h_2,b_2\\ h_1b_1-h_2b_2=k}}\mathbf{e}(t_1m)\mathbf{e}(t_2b_1)\mathbf{e}(t_3b_2)\mathbf{e}(t_4h_1)\mathbf{e}(t_5h_2)\Big|^2\\ &\le \sum_{k\sim K}\sum_{h_2,b_2}\tau(h_2b_2+k)\Big(\sum_{\substack{h_1,b_1,h_2,b_2\\ h_1b_1-h_2b_2=k}}1\Big)\\ &\le (HB+K)^{\varepsilon}H|\mathcal{B}|\sum_{h_1,b_1}\sum_{h_2,b_2}1 \ll H^3|\mathcal{B}|^3x^{3\varepsilon}\,.\end{aligned}$$

In order to estimate the 5-dimensional integral in question we consider for instance the integral

$$\int_{-\infty}^{\infty}(t_5H)^{-q_5}\,dt_5\,.$$

Let $q_5 = 0$ if $|t_5| \le 1/H$ and $q_5 = 2$ otherwise. Then it contributes the quantity

$$\int_{|t_5|\le H^{-1}}1\,dt_5 + \int_{|t_5|>H^{-1}}(t_5H)^{-2}\,dt_5 \le \frac{3}{H}\,.$$

Following the same arguments for the remaining $q_i,\ i = 1,\ldots,4$, we obtain

$$\begin{aligned}&E(H,K,S,M)\\ &\ll RM^{1/2}(H|\mathcal{B}|)^{3/2}[1+(1+X^{-1})^{1/2}(X+\sqrt{M})(X+\sqrt{K})]x^{2\varepsilon}\\ &\ll RM^{1/2}(H|\mathcal{B}|)^{3/2}\left\{\left(1+\frac{S}{\sqrt{MK}}\right)^{1/2}\sqrt{MK}\left(1+\sqrt{\frac{M}{S^2}}\right)\left(1+\sqrt{\frac{K}{S^2}}\right)\right\}x^{2\varepsilon}\\ &\ll RM^{1/2}(H|\mathcal{B}|)^{3/2}\left(1+\frac{S}{\sqrt{MK}}\right)^{1/2}\sqrt{MK}x^{3\varepsilon}\end{aligned}$$

since in view of (16), $M \le S^2$ and $K \le S^2x^{2\varepsilon}$. Therefore by (14) and (16) we obtain

$$T_e(x,\mathcal{B},D) \ll \max_{H,K,S}(H|\mathcal{B}|)^{3/2}\{S\sqrt{K}(1+S/\sqrt{K})^{1/2}\}x^{11\varepsilon}\,.$$

Splitting the right-hand expression into two terms coming from the two terms of the sum $1+S/\sqrt{K}$ shows that $T_e(x,\mathcal{B},D) \ll T_1+T_2$ where

$$T_1 \ll \max_{H,K,S}(H|\mathcal{B}|)^{3/2}S\sqrt{K}x^{11\varepsilon}\,,\qquad T_2 \ll \max_{H,K,S}(H|\mathcal{B}|)^{3/2}S^{3/2}K^{1/4}x^{11\varepsilon}\,.$$

Hence by (16) we obtain

$$T_1 \ll (Dx^{-1}|\mathcal{B}|)^{3/2}[D(DB/x)]^{1/2}B^{3e/2}x^{14\varepsilon}$$

$$\ll D|\mathcal{B}|^2 B^{2e}[D^{3/2}|\mathcal{B}|^{-1/2}B^{1/2}x^{-2}]x^{14\varepsilon}\,,$$

which is admissible since

$$D \le x^{4/3}(|\mathcal{B}|/B)^{1/3}x^{-14\varepsilon}\,.$$

Finally,

$$\begin{aligned} T_2 &\ll \max_{\mathcal{S}}(Dx^{-1}|\mathcal{B}|)^{3/2}S^{3/2}(DB/x)^{1/4}B^{3e/2}x^{15\varepsilon} \\ &\ll (Dx^{-1}|\mathcal{B}|)^{3/2}D^{3/4}(DB/x)^{1/4}B^{3e/2}x^{15\varepsilon} \\ &\ll D|\mathcal{B}|^2B^{2e}\{D^{3/2}x^{-7/4}|\mathcal{B}|^{-1/2}B^{1/4}\}x^{15\varepsilon}\,, \end{aligned}$$

this being also admissible since

$$D \le x^{7/6}(|\mathcal{B}|^2/B)^{1/6}x^{-19\varepsilon}\,.$$

This completes the proof of (9) and hence the proof of the Theorem.

Acknowledgements. The author is grateful to the referee for his remarks that much simplified the final version of the paper.

REFERENCES

[1] E. Bombieri, J. B. Friedlander and H. Iwaniec, *Primes in arithmetic progressions to large moduli. II*, Math. Ann. 277 (1987), 361–393.

[2] J. M. Deshouillers and H. Iwaniec, *Kloosterman sums and Fourier coefficients of cusp forms*, Invent. Math. 70 (1982), 219–288.

[3] J. Friedlander and H. Iwaniec, *Quadratic polynomials and quadratic forms*, Acta Math. 141 (1978), 1–15.

[4] H. Iwaniec, *On sums of two norm from cubic fields*, in: Journées de théorie additive des nombres, Univ. de Bordeaux I, 1977, 71–89.

[5] —, *Rosser's sieve*, Acta Arith. 36 (1980), 171–202.

[6] —, *On the greatest prime factor of* $n^2 + 1$, Ann. Inst. Fourier (Grenoble) 32 (4) (1982), 1–11.

[7] H. Iwaniec and J. Pomykała, *Sums and differences of quartic norms*, Mathematika, to appear.

[8] J. Pomykała, *On the greatest prime divisor of quadratic sequences*, Sém. Théorie des Nombres Bordeaux 3 (1991), 361–375.

[9] H. J. S. Smith, *Report on the theory of numbers, Part III*, Report of the British Association for 1861, 292–340; reprinted in: The Collected Mathematical Papers of Henry John Stephen Smith, Vol. I, Chelsea, 1965, 163–228.

INSTITUTE OF MATHEMATICS
WARSAW UNIVERSITY
BANACHA 2
02-097 WARSZAWA, POLAND
E-mail: POMYKALA@MIMUW.EDU.PL

Reçu par la Rédaction le 13.12.1989;
en version modifiée le 15.4.1993