On Character Sums of Binary Quadratic Forms [1] [2]

Mei-Chu Chang[3]

Abstract.

We establish character sum bounds of the form

$$\Bigg|\sum_{\substack{a\le x\le a+H\\ b\le y\le b+H}}\chi(x^2+ky^2)\Bigg|<p^{-\tau}H^2,$$

where χ is a nontrivial character (mod p), $p^{\frac{1}{4}+\varepsilon}<H<p$, and $|a|,|b|<p^{\varepsilon/2}H$.

As an application, we obtain that given $k\in\mathbb{Z}\backslash\{0\}$, x^2+k is a quadratic non-residue (mod p) for some $1\le x<p^{\frac{1}{2\sqrt{e}}+\epsilon}$.

Introduction.

Let k be a nonzero integer. Let p be a large prime and let $H\le p$. We are interested in the character sum $\sum_{x,y}\chi(x^2+ky^2)$, where $\chi \pmod q$ is a nontrivial character, and x and y run over intervals of length H; say $a\le x\le a+H$ and $b\le y\le b+H$, and a and b are less than $p^{\epsilon}H$. The trivial bound for this character sum is H^2, and we seek an upper bound of the form $H^2p^{-\delta}$ for some $\delta>0$. Burgess [Bu3] considered such character sums, and obtained the desired $H^2p^{-\delta}$ estimate provided $H\ge p^{\frac{1}{3}+\epsilon}$. Moreover, in the case that x^2+ky^2 is irreducible (mod p) (i.e., $-k$ is a quadratic non-residue (mod p)), Burgess obtained such cancelation in the wider range $H\ge p^{\frac{1}{4}+\epsilon}$. In this paper we obtain a corresponding result in the case that x^2+ky^2 is reducible (mod p) (i.e., $-k$ is a quadratic residue (mod p)).

More precisely, we prove

Theorem. *Given $\varepsilon>0$, there is $\tau>0$ such that if p is a sufficiently large prime and H is an integer satisfying*

$$p^{\frac{1}{4}+\varepsilon}<H<p, \tag{0.1}$$

we have

[1]2000 *Mathematics Subject Classification.*Primary 11L40, 11L26; Secondary 11A07, 11B75.

[2]*Key words.* character sums, quadratic residues, Burgess

[3]Research partially financed by the National Science Foundation.

$$\left| \sum_{\substack{a \le x \le a+H \\ b \le y \le b+H}} \chi(x^2 + ky^2) \right| < p^{-\tau} H^2 \tag{0.2}$$

for any nontrivial character $\chi \pmod p$ *and arbitrary* $|a|, |b| < p^{\varepsilon/2} H$.

Our argument is a variant of Burgess' well-known method [Bu1]. Following [Bu2], this estimate for binary forms allows us to deduce

Corollary. *Given* $k \in \mathbb{Z} \backslash \{0\}$, *we have* $\left(\frac{x^2+k}{p}\right) = -1$ *for some* $1 < x < p^{\frac{1}{2\sqrt{e}}+\epsilon}$, *for all* $\epsilon > 0$.

In [Bu2], Burgess established this statement for $x < p^{\frac{2}{3\sqrt{e}}+\epsilon}$ and for $x < p^{\frac{1}{2\sqrt{e}}+\epsilon}$ provided $x^2 + k$ is assumed irreducible $\pmod p$. Thus, both the theorem and the corollary are only new if $-k$ is a quadratic residue $\pmod p$. The other case was treated by Burgess based on the following approach.

Recall that if $-k$ is a quadratic non-residue $\pmod p$, then $\chi(x^2+ky^2)$ is a character $\pmod p$ of $x+\omega y$ with $\omega = \sqrt{-k}$. Estimate (0.2) is then equivalent to bounding a character sum

$$\sum_{z \in B} \chi'(z) \tag{0.3}$$

where $B = \{x + \omega y : a \le x \le a + H, b \le y \le b + H\}$ and χ' is a nontrivial multiplicative character of $\mathbb{F}_{p^2}$. In [Bu5], Burgess established the desired bound for (0.3) assuming $H \ge p^{\frac{1}{4}+\epsilon}$. A more general result along these lines was obtained by A. Karacuba [Ka], for boxes $B \subset \mathbb{F}_{p^n}$ of the form

$$B = \{x_0 + x_1\omega + \cdots + x_{n-1}\omega^{n-1} : r_i \le x_i \le r_i + H, \text{ for } i = 0, \ldots, n-1\}.$$

Here ω is a root of a *given* polynomial of degree n, which is irreducible $\pmod p$ and assuming again $H > p^{\frac{1}{4}+\epsilon}$.

Notation.

- $[a, b] := \{i \in \mathbb{Z} : a \le i \le b\}$.
- $x \equiv y$ means $x \equiv y \pmod p$.

§1. Estimate of the character sums.

Denote $f(x, y) = x^2 + ky^2, k \in \mathbb{Z} \backslash \{0\}$ and assume

$$f(x, y) \equiv (x + \lambda y)(x - \lambda y), \ \lambda \in \mathbb{F}_p^*. \tag{1.1}$$

Recall also that by Weil's theorem

$$\max_{a\in\mathbb{F}_p^*}\Big|\sum_{x\in I}\chi(x^2+a)\Big| < c\sqrt{p}\ \log p \tag{1.2}$$

for χ a nontrivial character (mod p) and $I\subset[1,p)$ an interval. Hence

$$\Big|\sum_{\substack{a\le x\le a+H\\ b\le y\le b+H}}\chi(f(x,y))\Big| < c\sqrt{p}\ (\log p)H, \tag{1.3}$$

and we may therefore assume $H<p^{\frac{3}{4}}$.

Proof of the theorem.

We let $a=b=0$. The modification needed in the argument below to treat the situation $|a|,|b|<p^{\epsilon/2}H$ are straightforward and left to the reader.

As mentioned earlier, the basic technique is Burgess'.

Let

$$\delta=\frac{\varepsilon}{4}. \tag{1.4}$$

We introduce parameters

$$M=[p^\delta] \tag{1.5}$$

and

$$D=p^{\frac{1}{3}}H^{-\frac{1}{3}}<p^{-2\delta}H. \tag{1.6}$$

Here the inequality is because of (0.1).

Thus for all $0\le u,v\le D, 0\le t\le M$

$$S:=\sum_{0\le x,y\le H}\chi(f(x,y))=\sum_{0\le x,y\le H}\chi(f(x+ut,y+vt))+O(p^{-\delta}H^2). \tag{1.7}$$

Taking some subset $\mathcal{D}\subset[0,D]^2$, it follows that

$$|S|\le\frac{1}{|\mathcal{D}|M}\sum_{\substack{0\le x,y\le H\\ (u,v)\in\mathcal{D}}}\Big|\sum_{t=1}^{M}\chi(f(x+ut,y+vt))\Big|+O(p^{-\delta}H^2). \tag{1.8}$$

Assume $u+\lambda v, u-\lambda v\not\equiv 0$ for $(u,v)\in\mathcal{D}$. By (1.2), the first term in (1.8) equals

$$\begin{aligned}
&\frac{1}{|\mathcal{D}|M}\sum_{\substack{0\le x,y\le H\\(u,v)\in\mathcal{D}}}\Big|\sum_{t=1}^{M}\chi\Big(\Big(\frac{x+\lambda y}{u+\lambda v}+t\Big)\Big(\frac{x-\lambda y}{u-\lambda v}+t\Big)\Big)\Big|\\
=&\frac{1}{|\mathcal{D}|M}\sum_{\xi,\zeta\in\mathbb{F}_p} w_{\xi,\zeta}\ \Big|\sum_{t=1}^{M}\chi((\xi+t)(\zeta+t))\Big|,
\end{aligned}\tag{1.9}$$

where

$$w_{\xi,\zeta}=\Big|\Big\{(x,y,u,v)\in[0,H]^2\times\mathcal{D}:\frac{x+\lambda y}{u+\lambda v}=\xi \text{ and } \frac{x-\lambda y}{u-\lambda v}=\zeta\Big\}\Big|.$$

Let

$$r=\Big[\frac{10}{\varepsilon}\Big].\tag{1.10}$$

To estimate (1.9), we follow the usual approach of applying Hölder's inequality with suitable exponent $2r\in\mathbb{Z}_+$ and Weil's theorem later.

Thus, (1.9) is bounded by

$$\frac{1}{|\mathcal{D}|M}\Big(\sum_{\xi,\zeta}(w_{\xi,\zeta})^{\frac{2r}{2r-1}}\Big)^{1-\frac{1}{2r}}\Big(\sum_{\xi,\zeta}\Big|\sum_{t=1}^{M}\chi((\xi+t)(\zeta+t))\Big|^{2r}\Big)^{\frac{1}{2r}},$$

which is bounded by

$$\frac{1}{|\mathcal{D}|M}\Big(\sum w_{\xi,\zeta}\Big)^{1-\frac{1}{r}}\Big(\sum w_{\xi,\zeta}^2\Big)^{\frac{1}{2r}}\Bigg(\sum_{t_i}\Big(\sum_{\xi}\chi\frac{(\xi+t_1)\dots(\xi+t_r)}{(\xi+t_{r+1})\dots(\xi+t_{2r})}\Big)^2\Bigg)^{\frac{1}{2r}}$$

Here $i=1,\dots,2r$, $t_i\in[1,M]$ and $\xi\in\mathbb{F}_p$ such that $\xi+t_{r+1},\dots,\xi+t_{2r}$ are nonzero.

Now by Weil's theorem, (1.9) is bounded by

$$\frac{1}{|\mathcal{D}|M}(H^2|\mathcal{D}|)^{1-\frac{1}{r}}\Big(\sum w_{\xi,\zeta}^2\Big)^{\frac{1}{2r}}\big(r^{2r}M^rp^2+M^{2r}(2rp^{\frac{1}{2}})^2\big)^{\frac{1}{2r}}.\tag{1.11}$$

(From the definition of $w_{\xi,\zeta}$, we have $|\sum w_{\xi,\zeta}|=H^2\ |\mathcal{D}|$.)

By (1.4), (1.5) and (1.10), if

$$p>\Big(\frac{10}{\varepsilon}\Big)^{\frac{40}{3\varepsilon}},\tag{1.12}$$

then $p>r^{2r}M^{-r}p^2$. Therefore, by (1.8) and (1.11) (after canceling M), we have

$$|S|<H^2(H^2|\mathcal{D}|)^{-\frac{1}{r}}\Big(\sum w_{\xi,\zeta}^2\Big)^{\frac{1}{2r}}p^{\frac{1}{2r}}+O(p^{-\delta}H^2).\tag{1.13}$$

Our next aim is to estimate $\sum w_{\xi,\zeta}^2$, which is the number of solutions of the following system of equations in $\mathbb{F}_p$.

$$\frac{x_1+\lambda y_1}{u_1+\lambda v_1} \equiv \frac{x_2+\lambda y_2}{u_2+\lambda v_2}$$
$$\frac{x_1-\lambda y_1}{u_1-\lambda v_1} \equiv \frac{x_2-\lambda y_2}{u_2-\lambda v_2},$$

when $x_i, y_i \in [0,H]$ and $(u_i, v_i) \in \mathcal{D}$ for $i = 1, 2$.

Define

$$\mathcal{D} = \Big\{(u,v) \in \Big[\frac{D}{2}, D\Big]^2 : (u,v) = (u,k) = (v,k) = 1,\ u \pm \lambda v \not\equiv 0\Big\}.$$

(Here (u,v) denotes $\gcd(u,v)$.)

Hence

$$|\mathcal{D}| \sim D^2.$$

Multiplying and adding the equations in the above system, we get by (1.2)

$$(x_1^2 + ky_1^2)(u_2^2 + kv_2^2) \equiv (x_2^2 + ky_2^2)(u_1^2 + kv_1^2) \tag{1.14}$$
$$(x_1u_1 + ky_1v_1)(u_2^2 + kv_2^2) \equiv (x_2u_2 + ky_2v_2)(u_1^2 + kv_1^2). \tag{1.15}$$

We impose on H, D the condition

$$HD^3 < \frac{p}{8k^2}. \tag{1.16}$$

Hence (1.15) holds in $\mathbb{Z}$ and we have

$$(x_1u_1 + ky_1v_1)(u_2^2 + kv_2^2) = (x_2u_2 + ky_2v_2)(u_1^2 + kv_1^2). \tag{1.17}$$

Fix u_1, u_2, v_1, v_2 and let $\Delta = \gcd(u_1^2 + kv_1^2, u_2^2 + kv_2^2)$.

Hence

$$\begin{cases} u_1^2 + kv_1^2 = \Delta w_1 \\ u_2^2 + kv_2^2 = \Delta w_2 \end{cases}, \tag{1.18}$$

where $(w_1, w_2) = 1$.

Since a rational integer a has at most $\frac{\log a}{\log\log a} \log D$ factorizations of the form $x + y\lambda$ in $\mathbb{Q}(\lambda)$ with $x, y \in [0, D]$, the equation

$$u^2 + kv^2 = a$$

has at most $\exp\big(c\frac{\log(D+|a|)}{\log\log(D+|a|)}\big)$ solutions $(u,v) \in [0,D]^2$. Therefore, given w_1, w_2, Δ, the system (1.18) has $< p^{\varepsilon_1}$ solutions (u_1, v_1, u_2, v_2). It follows from (1.17) that

$$\begin{cases} x_1u_1 + ky_1v_1 = tw_1 \\ x_2u_2 + ky_2v_2 = tw_2 \end{cases} \tag{1.19}$$

for some $t \in \mathbb{Z}$, satisfying

$$|t| \leq \frac{HD}{|w_1| + |w_2|}. \tag{1.20}$$

Let x_1', y_1', x_2', y_2' be some solution (other than x_1, y_1, x_2, y_2) of (1.19) and (1.14) with specified u_1, v_1, u_2, v_2 and t. Then

$$\begin{cases} (x_1 - x_1')u_1 = k(y_1' - y_1)v_1 \\ (x_2 - x_2')u_2 = k(y_2' - y_2)v_2 \end{cases}. \tag{1.21}$$

Since $(u_1, kv_1) = 1 = (u_2, kv_2)$, we get

$$\begin{cases} x_1 - x_1' = s_1kv_1 \\ y_1' - y_1 = s_1u_1 \\ x_2 - x_2' = s_2kv_2 \\ y_2' - y_2 = s_2u_2 \end{cases}. \tag{1.22}$$

for some $s_1, s_2 \in \mathbb{Z}$ satisfying

$$|s_i| \leq \frac{H}{D} \quad \text{for } i = 1, 2. \tag{1.23}$$

Substituting (1.22) in (1.14) and (1.18) yield the following equation in s_1, s_2

$$w_2\big((x_1' + s_1kv_1)^2 + k(y_1' - s_1u_1)^2\big) \equiv w_1\big((x_2' + s_2kv_2)^2 + k(y_2' - s_2u_2)^2\big).$$

Hence

$$\Delta w_1w_2(s_1^2 - s_2^2) + 2w_2(x_1'v_1 - y_1'u_1)s_1 - 2w_1(x_2'v_2 - y_2'u_2)s_2 \equiv 0 \tag{1.24}$$

and there are obviously at most $c\frac{H}{D}$ solutions in (s_1, s_2) satisfying (1.23) and (1.24). Summarizing, we showed that for given Δ, w_1, w_2, the system of equations (1.14) and (1.15) has at most

$$p^{\varepsilon_1} \frac{HD}{|w_1| + |w_2|} \frac{H}{D} \tag{1.25}$$

solutions in x_1, y_1, x_2, y_2. Notice that by (1.18), $\Delta(|w_1| + |w_2|) \leq D^2$.

Summing (1.25) over Δ, w_1, w_2 we obtain

$$p^{\varepsilon_1} H^2 \sum_{1\le\Delta\le D^2} \sum_{|w_1|+|w_2|\le\frac{D^2}{\Delta}} \frac{1}{|w_1|+|w_2|} < p^{\varepsilon_1} H^2 \sum_{1\le\Delta\le D^2} \frac{D^2}{\Delta}$$
$$< p^{\varepsilon_1} H^2 D^2.$$

Therefore

$$\sum_{\xi,\zeta} w^2_{\xi,\zeta} < p^{\varepsilon_1} H^2 D^2, \tag{1.26}$$

provided H, D satisfy (1.16).

Substitute (1.26) in (1.13). By (0.1) and (1.6), we have

$$|S| < H^2 p^{-\varepsilon^2/15}. \qquad \square$$

With some small modification of the proof of the theorem, we can also obtain the following more general statement.

Theorem'. *Given $\varepsilon > 0$, there is $\tau > 0$ such that if p is a sufficiently large prime and H is an integer satisfying*

$$p^{\frac{1}{4}+\varepsilon} < H < p,$$

we have

$$\Bigg| \sum_{\substack{a\le x\le a+H\\ b\le y\le b+H}} \chi(x^2+ky^2) \Bigg| < p^{-\tau} H^2$$

for any nontrivial character $\chi(\mathrm{mod}\ p)$ and arbitrary $|a|, |b| < p^{\varepsilon/2} H$.

§2. An application to quadratic non-residues.

In this section we will prove the corollary.

Let $\phi(x) = x^2 + k$, with $k \in \mathbb{Z}\backslash\{0\}$ and let p be a large prime. Assume

$$\left(\frac{\phi(x)}{p}\right) = 1 \ for\ 1 \le x \le H. \tag{2.1}$$

The problem of estimating $H = H(p)$ was considered in Burgess' paper [Bu2]. (See also [Bu4].)

We distinguish the following two cases.

Case 1. $k = -\ell^2, \ell \in \mathbb{Z}$.

Hence $\phi(x) = (x+\ell)(x-\ell)$. In this case $H < p^{\frac{1}{4\sqrt{e}}+\epsilon}$. Indeed, if $\left(\frac{x+\ell}{p}\right) = \left(\frac{x-\ell}{p}\right)$ for $1 \le x \le H$, taking $x = \ell, 3\ell, 5\ell \ldots$, gives that $\left(\frac{2\ell\, y}{p}\right) = \text{constant for } 1 \le y < \frac{H}{2\ell}$. Hence $\left(\frac{y}{p}\right) = 1$, which contradicts

Burgess theorem [Bu1] on the existence of quadratic non-residues in short intervals $[1, p^{\frac{1}{4\sqrt{e}}+\epsilon}]$.

Case 2. $-k$ is not a square.

We will follow the argument in [Bu2] with some adjustment. We may assume $k > 0$, since the case $k < 0$ is similar. (See [Bu2].) For readers' convenience we state below the lemmas we use from [Bu2]. (See Lemmas 1, 3 in [Bu2].)

1. For $x, y \in \mathbb{Z}$, there exists a representation of $n = x^2 + ky^2$

$$n = u^2 \prod_{i=1}^{r} (v_i^2 + k)^{\alpha_i}, \tag{2.2}$$

for some $r \in \mathbb{N}$, positive integers $u, v_1, \ldots, v_r$ all $\leq n$ and $\alpha_i = \pm 1$.

2. Given $1 < \beta < \sqrt{e}$, there is a constant $M = M(\beta) > 0$ such that if

$$\Big(\frac{x^2 + ky^2}{p}\Big) = 1 \ for\ x^2 + ky^2 \leq H,$$

then for H sufficiently large and any prime $p > H^\beta$ we have

$$\sum_{x^2+ky^2 \leq H^\beta} \Big(\frac{x^2 + ky^2}{p}\Big) > MH^\beta,$$

where the sum is over all pairs x, y (not necessarily integers) for which $x + y\sqrt{-k}$ is an integer of $\mathbb{Q}(\sqrt{-k})$.

Since for $-k \equiv 3 \pmod 4$, $x + y\sqrt{-k}$ is an algebraic integer of $\mathbb{Q}(\sqrt{-k})$ if and only if $x, y \in \mathbb{Z}$, the sum is over all $x, y \in \mathbb{Z}$ with $x^2 + ky^2 \leq H^\beta$. For $-k \equiv 1 \pmod 4$ the ring of algebraic integers is generated by $\frac{1+\sqrt{-k}}{2}$. Burgess showed that the inequality holds when the sum is over all $x, y \in \mathbb{Z}$ such that $x^2 + 4ky^2 \leq H^\beta$. In both cases, the proofs of the theorem are identical, so we give only the former here.

It follows from our assumption (2.1) and (2.2) that

$$\Big(\frac{x^2 + ky^2}{p}\Big) = 1 \ \text{ if } \ x^2 + ky^2 \leq H. \tag{2.3}$$

Hence we may apply Burgess' second lemma and get a contradiction, if we show that

$$\sum_{x^2+ky^2 \leq H^\beta} \Big(\frac{x^2 + ky^2}{p}\Big) = O(p^{-\delta} H^\beta). \tag{2.4}$$

We divide the region enclosed by the ellipse $x^2 + ky^2 = H^\beta$ into squares of length h with $h > p^{1/4+\epsilon}$. For those squares completely lying in the ellipse, we use Theorem' to estimate the character sum.

For the others, we count the number of lattice points and use the trivial bound.

According to Theorem', it follows that (2.4) will hold provided $H^{\frac{\beta}{2}} > p^{\frac{1}{4}+\epsilon}$ for some $\epsilon > 0$. Therefore $H < p^{\frac{1}{2\sqrt{\epsilon}}}$. Hence the corollary is proved.

Acknowledgement. The author would like to thank the referee for helpful comment.

References

[Bu1] D.A. Burgess, *On character sums and primitive roots*, Proc LMS (3), 12, (1962), 179-192.

[Bu2] ———, *On the quadratic character of a polynomial*, JLMS, 42, (1967), 73-80.

[Bu3] ———, *A note on character sums of binary quadratic forms*, JLMS, 43 (1968), 271-274.

[Bu4] ———, *Direchlet characters and polynomials*, Trudy Math Inst-Steklov, 132, (1973).

[Bu5] ——— *Character sums and primitive roots in finite fields* , Proc. London Math. Soc. (3) 17 (1967), 11-25.

[Ka] A. A. Karacuba, *Estimates of character sums*, Izv. Akad Nauk SSR, Ser Mat Tom, 34, (1970), N1.

Department Of Mathematics, University Of California, Riverside, CA 92521

E-mail address: mcc@math.ucr.edu