SMALL SOLUTIONS OF THE CONGRUENCE $ax^2 + by^2 \equiv c(\mathrm{mod}\ k)$

Kenneth S. Williams*

(received February 22, 1969)

1. Introduction. In 1957, Mordell [3] proved

THEOREM. *If* p *is an odd prime there exist non-negative integers* $x, y \leq A p^{3/4} \log p$, *where* A *is a positive absolute constant, such that*

$$(1.1) \qquad ax^2 + by^2 \equiv c(\mathrm{mod}\ p),$$

provided $(abc, p) = 1$.

Recently Smith [5] has obtained a sharp asymptotic formula for the sum $\Sigma\{r(n) : n \leq X,\ n \equiv c(\mathrm{mod}\ k)\}$ where $r(n)$ denotes the number of representations of n as the sum of two squares. As an application of the asymptotic formula for this sum, he deduced

THEOREM. *If* k *is an odd integer, containing only a bounded number of factors, there exist non-negative integers* $x, y \leq B k^{3/4}$, *where* B *is a positive absolute constant, such that*

$$(1.2) \qquad x^2 + y^2 \equiv c(\mathrm{mod}\ k),$$

provided $(c, k) = 1$.

This sharpens Mordell's result when $a = b = 1$ and $k = p$. It is the purpose of this paper to generalize Smith's result to the case of the congruence $ax^2 + by^2 \equiv c(\mathrm{mod}\ k)$. We use an entirely different method from that of Smith. We apply an idea due to Tietäväinen [7]. We prove

THEOREM. *If* k *is an odd integer there exist non-negative integers* $x, y \leq C k^{3/4} d(k)^{1/2}$, *where* C *is a positive absolute constant and* $d(k)$ *denotes the number of divisors of* k, *such that*

*This research was supported by NRC Grant A-7233.

Canad. Math. Bull. vol. 12, no. 3, 1969

https://doi.org/10.4153/CMB-1969-039-0 Published online by Cambridge University Press

(1.3) $$ax^2 + by^2 \equiv c \pmod{k},$$

provided $(abc, k) = 1$.

Smith's result is the special case $a = b = 1$, $d(k)$ bounded.

2. Notation. We let

(2.1) $$h = [D\, k^{3/4}\, d(k)^{1/2}] + 1,$$

where $D > 0$ is defined by

(2.2) $$D^2 = \sum_{d=1}^{\infty} \frac{1}{d^{3/2}}.$$

Clearly $h \geq 1$ and k is supposed to be large enough so that $h \leq \frac{1}{2}(k - 1)$. For any integer x we let $N(k, x)$ denote the number of solutions (u, v) of

(2.3) $$u + v \equiv x \pmod{k},$$

with

(2.4) $$1 \leq u \leq h, \qquad 1 \leq v \leq h.$$

Clearly

(2.5) $$\sum_{x=0}^{k-1} N(k, x) = h^2.$$

For any real number u we write

(2.6) $$e(u) \equiv \exp(2\pi i u)$$

and it is well known that for any integer r we have

$$(2.7)\qquad \frac{1}{k}\sum_{t=0}^{k-1} e\left(\frac{rt}{k}\right) = \begin{cases} 1, & \text{if } r \equiv 0 \pmod{k}, \\ 0, & \text{if } r \not\equiv 0 \pmod{k}. \end{cases}$$

We also define for arbitrary integers r and s :

$$(2.8)\qquad M(k, r) = \sum_{x=0}^{k-1} N(k, x)\; e\left(\frac{rx^2}{k}\right),$$

$$(2.9)\qquad A(k, r) = \sum_{x=1}^{h} e\left(\frac{rx}{k}\right),$$

$$(2.10)\qquad T(k, r, s) = \sum_{x=0}^{k-1} e\left(\frac{rx^2 + sx}{k}\right),$$

$$(2.11)\qquad S(k, r) = T(k, r, 0),$$

$$(2.12)\qquad K(k, r, s) = \sum_{\substack{x=1 \\ (x, k)=1}}^{k-1} e\left(\frac{rx + s[x, k]}{k}\right),$$

where $[x, k]$ denotes the unique integer m satisfying

$$(2.13)\qquad xm \equiv 1 \pmod{k}, \quad 1 \leq m \leq k-1, \quad \text{for } (x, k) = 1.$$

The sum $A(k, r)$ (considered by Tietäväinen [6] when k is prime) satisfies

$$(2.14)\qquad \sum_{r=0}^{k-1} |A(k, r)|^2 = kh.$$

The sums $T(k, r, s)$ and $S(k, r)$ are Gaussian sums and it is well known that (see for example [2])

$$(2.15)\qquad T(k, r, s) = \begin{cases} 0, & \text{if } s \not\equiv 0 \pmod{d}, \\ d\, T\left(\frac{k}{d}, \frac{r}{d}, \frac{s}{d}\right), & \text{if } s \equiv 0 \pmod{d}, \end{cases}$$

https://doi.org/10.4153/CMB-1969-039-0 Published online by Cambridge University Press

where $d = (k, r)$. Also if $(k, r) = 1$, with k odd, we have

$$(2.16) \qquad T(k, r, s) = e\left(\frac{-[4, k] \ s^2[r, k]}{k}\right) S(k, r)$$

and (see for example [4])

$$(2.17) \qquad S(k, r) = \left(\frac{r}{k}\right)_J i^{\frac{1}{4}(k-1)^2} k^{1/2}$$

where $\left(\frac{r}{k}\right)_J$ is the Jacobi symbol. Finally $K(k, r, s)$ is the Kloosterman sum, which Estermann [1] has shown satisfies

$$(2.18) \qquad |K(k, r, s)| \le d(k) \ k^{1/2} \ (r, s, k)^{1/2} .$$

This estimate is a consequence of the work of Weil [8].

3. Idea of proof. The idea of the proof is to show that

$$(3.1) \qquad \sum_{\substack{x, y=0 \\ ax^2 + by^2 \equiv c \pmod k}}^{k-1} N(k, x) \, N(k, y) > 0 .$$

This result implies that there exist integers x and y $(0 \le x, y \le k-1)$ such that

$$(3.2) \qquad ax^2 + by^2 \equiv c \pmod k$$

and

$$(3.3) \qquad N(k, x) > 0, \quad N(k, y) > 0 .$$

The conditions (3.3) imply the existence of integers u, v, u', v' such that

$$(3.4) \qquad 1 \le u, v, u', v' \le h \le \frac{k-1}{2}$$

and

$$(3.5) \qquad u + v \equiv x, \; u' + v' \equiv y \pmod{k} .$$

Hence

$$|x - (u+v)| \le k-1, \qquad |y - (u'+v')| \le k-1$$

and so

$$(3.6) \qquad \begin{cases} 0 < x = u + v \le 2h = 2[Dk^{3/4} d(k)^{1/2}] + 2 \le Ck^{3/4} d(k)^{1/2}, \\ 0 < y = u' + v' \le 2h = 2[Dk^{3/4} d(k)^{1/2}] + 2 \le Ck^{3/4} d(k)^{1/2}, \end{cases}$$

for a suitable positive absolute constant $C \le 2\sqrt{3} + 2$. This is the required result.

4. Proof of theorem. From (2.7) we have

$$\sum_{t=0}^{k-1} e\left\{\frac{(ax^2 + by^2 - c)t}{k}\right\} = \begin{cases} k, & \text{if } ax^2 + by^2 \equiv c \pmod{k}, \\ 0, & \text{otherwise}, \end{cases}$$

so that

$$k \sum_{\substack{x, y=0 \\ ax^2 + by^2 \equiv c \pmod{k}}}^{k-1} N(k,x) \; N(k,y)$$

$$= \sum_{x,y=0}^{k-1} N(k,x) \; N(k,y) \sum_{t=0}^{k-1} e\left\{\frac{(ax^2 + by^2 - c)t}{k}\right\}$$

$$= \left\{\sum_{x=0}^{k-1} N(k,x)\right\}^2 + \sum_{t=1}^{k-1} e\left(\frac{-ct}{k}\right) M(k, at) \, M(k, bt) ,$$

https://doi.org/10.4153/CMB-1969-039-0 Published online by Cambridge University Press

on picking out the term with $t = 0$. Thus from (2.5) we have

$$(4.1)\quad \left| k \sum_{\substack{x, y=0 \\ ax^2+by^2 \equiv c(\text{mod } k)}}^{k-1} N(k, x)\, N(k, y) - h^4 \right| = \left| \sum_{t=1}^{k-1} e\left(\frac{-ct}{k}\right) M(k, at)\, M(k, bt) \right|$$

Now

$$M(k, at) = \sum_{x=0}^{k-1} N(k, x)\, e\left(\frac{at\, x^2}{k}\right)$$

$$= \frac{1}{k} \sum_{x=0}^{k-1} \sum_{u, v=1}^{h} \sum_{r=0}^{k-1} e\left(\frac{r(u+v-x) + at\, x^2}{k}\right)$$

$$= \frac{1}{k} \sum_{r=0}^{k-1} \{A(k, r)\}^2\, T(k, at, -r),$$

so that

$$\sum_{t=1}^{k-1} e\left(\frac{-ct}{k}\right) M(k, at)\, M(k, bt)$$

$$= \frac{1}{k^2} \sum_{d|k} \sum_{\substack{t=1 \\ (t, k)=d}}^{k-1} \sum_{r, s=0}^{k-1} A(k, r)\}^2 \{A(k, s)\}^2\, T(k, at, -r)\, T(k, bt, -s)\, e\left(\frac{-ct}{k}\right)$$

$$= \frac{1}{k^2} \sum_{d|k} \sum_{\substack{r, s=0 \\ d|r, d|s}}^{k-1} \{A(k, r)\}^2 \{A(k, s)\}^2 \sum_{\substack{t=1 \\ (t, k)=d}}^{k-1} e\left(\frac{-ct}{k}\right) T(k, at, -r)\, T(k, bt, -s),$$

as $T(k, at, -r)\, T(k, bt, -s)$ is zero (see (2.15)) unless $-r \equiv 0\,(\text{mod}(k, at))$ and $-s \equiv 0\,(\text{mod}(k, bt))$, that is, unless $d|r$ and $d|s$, since $(ab, k) = 1$. In this case

$$T(k, at, -r) = d\, T\left(\frac{k}{d}, \frac{at}{d}, \frac{-r}{d}\right)$$

https://doi.org/10.4153/CMB-1969-039-0 Published online by Cambridge University Press

and

$$T(k, bt, -s) = d\, T\left(\frac{k}{d}, \frac{bt}{d}, \frac{-s}{d}\right)$$

so that the sum becomes

$$(4.2) \quad \frac{1}{k^2} \sum_{d|k} d^2 \sum_{\substack{r,s=0 \\ d|r;\, d|s}}^{k-1} \{A(k,r)\}^2 \{A(k,s)\}^2 \sum_{\substack{t=1 \\ (t,k)=d}}^{k-1} e\left(\frac{-ct}{k}\right) T\left(\frac{k}{d}, \frac{at}{d}, \frac{-r}{d}\right) T\left(\frac{k}{d}, \frac{bt}{d}, \frac{-s}{d}\right).$$

We next change the summation over t in (4.2) into summation over u, where $u = t/d$, which gives:

$$(4.3) \quad \frac{1}{k^2} \sum_{d|k} d^2 \sum_{\substack{r,s=0 \\ d|r,\, d|s}}^{k-1} \{A(k,r)\}^2 \{A(k,s)\}^2 \sum_{\substack{u=1 \\ (u, \frac{k}{d})=1}}^{\frac{k}{d}-1} e\left(\frac{-cu}{k/d}\right) T\left(\frac{k}{d}, au, \frac{-r}{d}\right) T\left(\frac{k}{d}, bu, \frac{-s}{d}\right).$$

From (2.16) and (2.17) the sum over u in (4.3) is

$$\sum_{\substack{u=1 \\ \left(u, \frac{k}{d}\right)=1}}^{\frac{k}{d}-1} e\left(\frac{-cu}{k/d}\right) e\left(\frac{-[4, k/d]\,(-r/d)^2\,[au, k/d]}{k/d}\right) \left(\frac{au}{k/d}\right)_J i^{\frac{1}{4}\left(\frac{k}{d}-1\right)^2} \left(\frac{k}{d}\right)^{1/2}$$

$$\cdot\ e\left(\frac{-[4, k/d]\,(-s/d)^2\,[bu, k/d]}{k/d}\right) \left(\frac{bu}{k/d}\right)_J i^{\frac{1}{4}\left(\frac{k}{d}-1\right)^2} \left(\frac{k}{d}\right)^{1/2}$$

$$= \frac{k}{d} \left(\frac{-ab}{k/d}\right)_J K\left(\frac{k}{d}, -c, -e\right),$$

where

$$e = [4a, k/d]\left(\frac{r}{d}\right)^2 + [4b, k/d]\left(\frac{s}{d}\right)^2 .$$

https://doi.org/10.4153/CMB-1969-039-0 Published online by Cambridge University Press

From (2.18)

$$|K(k/d, -c, -e)| \leq d(k/d) \left(\frac{k}{d}\right)^{1/2} (-c, -e, k/d)^{1/2} = d(k/d) \frac{k^{1/2}}{d^{1/2}},$$

as $(c, k) = 1$.

Hence

$$\left| \sum_{t=1}^{k-1} e\left(\frac{-ct}{k}\right) M(k, at) \; M(k, bt) \right|$$

$$\leq \frac{1}{k^2} \sum_{d|k} d^2 \sum_{\substack{r,\, s=0 \\ d|r,\, d|s}}^{k-1} |A(k, r)|^2 \, |A(k, s)|^2 \cdot \frac{k}{d} \cdot d(k/d) \frac{k^{1/2}}{d^{1/2}}$$

$$\leq \frac{d(k)}{k^{1/2}} \sum_{d|k} d^{1/2} \left\{ \sum_{\substack{r=0 \\ d|r}}^{k-1} |A(k, r)|^2 \right\}^2$$

$$= \frac{d(k)}{k^{1/2}} \sum_{d|k} d^{1/2} \left\{ \sum_{t=0}^{\frac{k}{d}-1} |A(k/d, t)|^2 \right\}^2$$

$$= \frac{d(k)}{k^{1/2}} \sum_{d|k} d^{1/2} \left(\frac{k}{d} \cdot h\right)^2$$

$$= d(k) k^{3/2} \; h^2 \sum_{d|k} \frac{1}{d^{3/2}}$$

$$< d(k) \; k^{3/2} \; h^2 \; D^2 .$$

Thus from (4.1)

https://doi.org/10.4153/CMB-1969-039-0 Published online by Cambridge University Press

$$k \sum_{\substack{x, y=0 \\ ax^2+by^2 \equiv c \pmod k}}^{k-1} N(k, x)\, N(k, y) > h^2 (h^2 - d(k)k^{3/2} D^2) > 0 ,$$

as $h = [D k^{3/4} d(k)^{1/2}] + 1 > D k^{3/4} d(k)^{1/2}$. This completes the proof of the theorem.

5. Conclusion. As remarked by Smith [5] it would be of great interest to know if the exponent $3/4$ of the theorem can be lowered. It would also be of interest to know if the method of this paper could be adapted to give a corresponding result for the congruence

$$ax^{\ell} + by^{m} \equiv c \pmod k) , \tag{5.1}$$

where $\ell \geq 2$, $m \geq 3$ and $(abc, k) = 1$.

REFERENCES

1. T. Estermann, On Kloosterman's Sum. Mathematika 8 (1961) 83-86.

2. T. Estermann, A new application of the Hardy-Littlewood-Kloostermann Method. Proc. Lond. Math. Soc. 12 (1962) 425-444.

3. L.J. Mordell, On the number of solutions in incomplete residue sets of quadratic congruences. Archiv der Math. 8 (1957) 153-157.

4. H. Rademacher, Lectures on Elementary Number Theory. (Blaisdell, 1964) 93.

5. R.A. Smith, The circle problem in an arithmetic progression. Canad. Math. Bull. 11 (1968) 175-184.

6. A. Tietäväinen, On the trace of a polynomial over a finite field. Ann. Univ. Turku., Ser. AI, 87 (1966) 3-7.

https://doi.org/10.4153/CMB-1969-039-0 Published online by Cambridge University Press

7. A. Tietäväinen, On non-residues of a polynomial. Ann. Univ. Turku., Ser. Al, 94 (1966) 3-6.

8. A. Weil, On some exponential sums. Proc. Nat. Acad. Sci. (U.S.A.) 34 (1948) 204-207.

Carleton University