Proc. Camb. Phil. Soc. (1971), **70**, 409
PCPS 70–43
Printed in Great Britain

Small solutions of the congruence

$a_1x_1^{l_1}+a_2x_2^{l_2}+a_0 \equiv 0 \pmod p$

BY KENNETH S. WILLIAMS†
Carleton University, Ottawa, Canada

(*Received* 12 *January* 1971)

1. *Introduction.* Throughout this paper a_0, a_1, a_2, l_1, l_2 denote *fixed* integers with $l_1 \geqslant 2$, $l_2 \geqslant 2$. We let $l = \max(l_1, l_2)$ and let P be the set of primes $p \nmid a_0, a_1, a_2$. Mordell (4) has shown that for any sufficiently large prime p the congruence

$$f(x_1,x_2) = a_1x_1^{l_1}+a_2x_2^{l_2}+a_0 \equiv 0 \pmod p \tag{1·1}$$

is soluble. Thus there are at most a finite number of such p for which (1·1) is insoluble. If there is at least one prime $p \in P$ for which (1·1) is insoluble, we let p_0 denote the largest of such p, so that (1·1) is soluble for all $p \in P$ with $p > p_0$ but not for $p = p_0$. Otherwise (1·1) is soluble for all $p \in P$ and we let $p_0 = 1$. From the work of Mordell (4) we have

$$p_0 \leqslant l_1 l_2 (l_1+1)(l_2+1). \tag{1·2}$$

For $p \in P$ with $p > p_0$ (1·1) is thus always soluble and any such solution (x_1, x_2) can be taken to satisfy

$$1 \leqslant x_i \leqslant p \quad (i = 1, 2). \tag{1·3}$$

Chalk (2) has posed the problem of estimating a 'small' solution of (1·1), at least for p sufficiently large; that is a solution for which p in the inequality (1·3) can be replaced by something less than p. Smith (5) has shown that for p sufficiently large there is always a solution satisfying $1 \leqslant x_i \ll p^{\frac{3}{4}} \log p$ $(i = 1, 2)$. It is the purpose of this paper to prove the following sharper and more precise result.

THEOREM. *If* $p(\in P) > p_0$ *there is a solution* (x_1, x_2) *of* (1·1) *satisfying*

$$1 \leqslant x_i \leqslant \min(p, 3(l+1)p^{\frac{3}{4}}) \quad (i = 1, 2).$$

We remark that this theorem contains nothing new if $p(\in P)$ is such that

$$p_0 < p < 3^4(l+1)^4,$$

since for such p we have $\quad p^{\frac{1}{4}} < 3(l+1), \quad p < 3(l+1)p^{\frac{3}{4}},$

giving

$$\min(p, 3(l+1)p^{\frac{3}{4}}) = p.$$

Hence in the proof of the theorem we can suppose that $p \geqslant 3^4(l+1)^4$. The proof uses an idea due to Tietäväinen (6) and a recent estimate of Bombieri (1) (see also (3)).

2. *Notation.* For any real number u we write

$$e(u) = \exp(2\pi i u/p)$$

so that if r is any integer we have

$$\frac{1}{p}\sum_{s=0}^{p-1} e(rs) = \begin{cases} 1, & \text{if } \; r \equiv 0 \pmod p, \\ 0, & \text{if } \; r \not\equiv 0 \pmod p. \end{cases} \tag{2·1}$$

† This research was supported by a National Research Council of Canada grant (No. A-7233).

We let
$$k = [\sqrt{2(l+1)}\,p^{\frac{3}{4}}]+1. \tag{2·2}$$
Now $p \geqslant 3^4(l+1)^4$ so that
$$\begin{aligned} p^{\frac{3}{4}}(p^{\frac{1}{4}}-2\sqrt{2(l+1)}) &\geqslant 3^3(l+1)^3\{3(l+1)-2\sqrt{2}(l+1)\} \\ &= (3-2\sqrt{2})\,3^3(l+1)^4 \\ &> \frac{1}{3^2}\cdot 3^3 \\ &= 3, \end{aligned}$$
and so we have
$$\begin{aligned} p &> 2\sqrt{2(l+1)}\,p^{\frac{3}{4}}+3 \\ &\geqslant 2[\sqrt{2(l+1)}\,p^{\frac{3}{4}}]+3 \\ &= 2k+1, \end{aligned}$$
giving
$$1 \leqslant k \leqslant \tfrac{1}{2}(p-1). \tag{2·3}$$
For $i = 1, 2$, we let $N(x_i)$ denote the number of solutions (u_{i1}, u_{i2}) of
$$u_{i1}+u_{i2} \equiv x_i \pmod p$$
with
$$1 \leqslant u_{ij} \leqslant k \quad (j = 1, 2).$$
Appealing to (2·1) we have
$$N(x_i) = \frac{1}{p}\sum_{u_{i1},u_{i2}=1}^{k}\sum_{s_i=0}^{p-1} e((u_{i1}+u_{i2}-x_i)\,s_i). \tag{2·4}$$
We also define for any integer r
$$A(r) = \sum_{s=1}^{k} e(rs) \tag{2·5}$$
so that
$$A(0) = k. \tag{2·6}$$
From (2·1), (2·3) and (2·5) we have
$$\sum_{r=0}^{p-1} |A(r)|^2 = pk. \tag{2·7}$$

3. *Proof of theorem.* For $i = 1, 2$ and $t = 0, 1, \ldots, p-1$, from (2·4) and (2·5), we have
$$\begin{aligned} \sum_{x_i=1}^{p} N(x_i)\,e(a_i t x_i^{l_i}) &= \frac{1}{p}\sum_{x_i=1}^{p}\sum_{u_{i1},u_{i2}=1}^{k}\sum_{s_i=0}^{p-1} e((u_{i1}+u_{i2}-x_i)\,s_i + a_i t x_i^{l_i}) \\ &= \frac{1}{p}\sum_{s_i=0}^{p-1}\{A(s_i)\}^2\sum_{x_i=1}^{p} e(a_i t x_i^{l_i}-s_i x_i). \end{aligned}$$
Hence we have
$$\begin{aligned} &\sum_{t=0}^{p-1} e(a_0 t)\left\{\sum_{x_1=1}^{p} N(x_1)\,e(a_1 t x_1^{l_1})\right\}\left\{\sum_{x_2=1}^{p} N(x_2)\,e(a_2 t x_2^{l_2})\right\} \\ &= \frac{1}{p^2}\sum_{s_1,s_2=0}^{p-1}\{A(s_1)\}^2\{A(s_2)\}^2\sum_{x_1,x_2=1}^{p} e(-s_1x_1-s_2x_2)\sum_{t=0}^{p-1} e(t(a_1x_1^{l_1}+a_2x_2^{l_2}+a_0)) \\ &= \frac{1}{p}\sum_{s_1,s_2=0}^{p-1}\{A(s_1)\}^2\{A(s_2)\}^2\sum_{\substack{x_1,x_2=1\\ f(x_1,x_2)\equiv 0 \\ (\mathrm{mod}\ p)}}^{p} e(-s_1x_1-s_2x_2). \end{aligned}$$

In this sum the terms with $(s_1, s_2) = (0,0)$ contribute (recall (2·6))

$$\frac{1}{p}\{A(0)\}^4 \sum_{\substack{x_1,x_2=1\\ f(x_1,x_2)\equiv 0\\ (\mathrm{mod}\ p)}}^{p} 1 = \frac{k^4}{p}N_p,$$

where N_p denotes the number of (x_1, x_2) with $1 \leqslant x_i \leqslant p$, $i = 1, 2$, satisfying (1·1). By a result of Mordell (4) N_p satisfies

$$|N_p - p| \leqslant p^{\frac{1}{2}}\{l_1(l_1+1)\,l_2(l_2+1)\}^{\frac{1}{2}}$$

so that

$$N_p \geqslant p-(l+1)^2p^{\frac{1}{2}}.$$

By a recent result of Bombieri (1), see also (3), as $f(x_1,x_2)$ is absolutely irreducible (mod p), for the terms with $(s_1,s_2) \neq (0,0)$ we have

$$\left|\sum_{\substack{x_1,x_2=1\\ f(x_1,x_2)\equiv 0\\ (\mathrm{mod}\ p)}}^{p} e(-s_1x_1-s_2x_2)\right| \leqslant (l^2+2l-3)\,p^{\frac{1}{2}}+l^2.$$

As $p \geqslant 3^4(l+1)^4 > l^4$, we have $(l^2+2l-3)\,p^{\frac{1}{2}}+l^2 < (l^2+2l-2)\,p^{\frac{1}{2}}$, and so

$$\begin{aligned}
&\left|\frac{1}{p}\sum_{\substack{s_1,s_2=0\\ (s_1,s_2)\neq(0,0)}}^{p-1}\{A(s_1)\}^2\{A(s_2)\}^2\sum_{\substack{x_1,x_2=1\\ f(x_1,x_2)\equiv 0\\ (\mathrm{mod}\ p)}}^{p} e(-s_1x_1-s_2x_2)\right|\\
&\qquad < \frac{(l^2+2l-2)}{p^{\frac{1}{2}}}\left\{\sum_{s=0}^{p-1}|A(s)|^2\right\}^2\\
&\qquad = (l^2+2l-2)\,p^{\frac{3}{2}}k^2,
\end{aligned}$$

using (2·7).

On the other hand we have

$$\begin{aligned}
&\sum_{=0}^{p-1} e(a_0t)\left\{\sum_{x_1=1}^{p} N(x_1)\,e(a_1tx_1^{l_1})\right\}\left\{\sum_{x_2=1}^{p} N(x_2)\,e(a_2tx_2^{l_2})\right\}\\
&\quad = \sum_{x_1,x_2=1}^{p} N(x_1)\,N(x_2)\sum_{t=0}^{p-1} e((a_1x_1^{l_1}+a_2x_2^{l_2}+a_0)\,t)\\
&\quad = p\sum_{\substack{x_1,x_2=1\\ f(x_1,x_2)\equiv 0\\ (\mathrm{mod}\ p)}}^{p} N(x_1)\,N(x_2),
\end{aligned}$$

and so

$$p\sum_{\substack{x_1,x_2=1\\ f(x_1,x_2)\equiv 0\\ (\mathrm{mod}\ p)}}^{p} N(x_1)\,N(x_2) > \frac{k^4}{q}(p-(l+1)^2p^{\frac{1}{2}}) - (l^2+2l-2)\,p^{\frac{3}{2}}k^2,$$

$$\begin{aligned}
f(x_1,x_2) &\equiv 0 \pmod p\\
&= k^4-(l+1)^2p^{-\frac{1}{2}}k^4-(l^2+2l-2)\,p^{\frac{3}{2}}k^2\\
&> k^4-(l+1)^2p^{\frac{3}{2}}k^2-(l^2+2l-2)\,p^{\frac{3}{2}}k^2 \quad (\text{as } k < p)\\
&= k^2\{k^2-(2l^2+4l-1)\,p^{\frac{3}{2}}\}\\
&> k^2\{2(l+1)^2p^{\frac{3}{2}}-(2l^2+4l-1)\,p^{\frac{3}{2}}\} \quad (\text{as } k > \sqrt{2}(l+1)\,p^{\frac{3}{4}})\\
&= 3k^2p^{\frac{3}{2}}\\
&> 0.
\end{aligned}$$

Hence there exist integers x_1 and x_2 ($1 \leqslant x_1, x_2 \leqslant p$) such that

$$f(x_1, x_2) \equiv 0 \pmod{p}$$

and
$$N(x_1) > 0, \quad N(x_2) > 0. \tag{3·1}$$

The conditions (3·1) imply the existence of integers $u_{11}, u_{12}, u_{21}, u_{22}$ such that

$$1 \leqslant u_{11}, \quad u_{12}, \quad u_{21}, \quad u_{22} \leqslant k \leqslant \frac{p-1}{2}$$

and
$$u_{11} + u_{12} \equiv x_1, \quad u_{21} + u_{22} \equiv x_2 \pmod{p}.$$

Hence we have

$$|x_1 - (u_{11} + u_{12})| \leqslant p - 1, \quad |x_2 - (u_{21} + u_{22})| \leqslant p - 1$$

and so for $i = 1, 2$ we have

$$1 \leqslant x_i = u_{i1} + u_{i2} \leqslant 2k = 2[\sqrt{2}(l+1)p^{\frac{3}{4}}] + 2.$$

This proves the theorem, as

$$2[\sqrt{2}(l+1)p^{\frac{3}{4}}] + 2 \leqslant 2\sqrt{2}(l+1)p^{\frac{3}{4}} + 2 \leqslant 3(l+1)p^{\frac{3}{4}},$$

since
$$(3 - 2\sqrt{2})(l+1)p^{\frac{3}{4}} > \tfrac{1}{9}.3^3(l+1)^4 > 2.$$

4. *Conclusion.* It would be interesting to know if the exponent $\frac{3}{4}$ in the theorem can be replaced by something smaller.

REFERENCES

(1) BOMBIERI, E. On exponential sums in finite fields. *Amer. J. Math.* **88** (1966), 71–105.

(2) CHALK, J. H. H. The number of solutions of congruences in incomplete residue systems. *Canad. J. Math.* **15** (1963), 291–296.

(3) CHALK, J. H. H. and SMITH, R. A. On Bombieri's estimate for exponential sums. *Acta Arith.* (to appear).

(4) MORDELL, L. J. The number of solutions of some congruences in two variables. *Math. Zeit.* **37** (1933), 193–209.

(5) SMITH, R. A. The distribution of rational points on hypersurfaces defined over a finite field. *Mathematika* **17** (1970), 328–332.

(6) TIETÄVÄINEN, A. On non-residues of a polynomial. *Ann. Univ. Turku., Ser. A I* **94** (1966), 3–6.