SMALL SOLUTIONS OF CUBIC CONGRUENCES

TODD COCHRANE

(Communicated by William W. Adams)

ABSTRACT. Let $C(\mathbf{x})$ be a cubic form in n variables over $\mathbf{Z}$ and p be a prime. Then for $0 < \sigma < \frac{2}{3}$ the congruence $C(\mathbf{x}) \equiv 0 \pmod{p}$ has a nonzero solution $\mathbf{x}$ with $\max |x_i| \ll p^{1/3+\sigma}$, provided that $n > 8/\sigma$, (where the constant in the $\ll$ depends on n and σ).

Let p be a prime and $F_1(\mathbf{x}), \dots, F_r(\mathbf{x})$ be forms of odd degrees $\leq d$ over $\mathbf{Z}$ where $\mathbf{x} = (x_1, x_2, \dots, x_n)$. Let $|\mathbf{x}| = \max_{1 \leq i \leq n} |x_i|$ and let $\mathbf{F}_p$ denote the finite field in p elements. In [4, Theorem 3] Schmidt proves that the system of congruences

$$(1) \quad F_1(\mathbf{x}) \equiv F_2(\mathbf{x}) \equiv \dots \equiv F_r(\mathbf{x}) \equiv 0 \pmod{p}$$

has a nonzero solution $\mathbf{x}$ with $|\mathbf{x}| \ll p^{1/3+\sigma}$ provided that $n > c(r, d)/\sigma^2$, where $c(r, d)$ is an explicitly given constant depending only on r and d . In this paper we employ the ideas of Schmidt to obtain a refinement of this result in the case of a single cubic form.

Theorem. Let $C(\mathbf{x})$ be a cubic form over $\mathbf{Z}$ and p be a prime. Then for $0 < \sigma \leq \frac{2}{3}$ the congruence $C(\mathbf{x}) \equiv 0 \pmod{p}$ has a nonzero solution $\mathbf{x}$ with $|\mathbf{x}| \ll p^{1/3+\sigma}$ provided that $n > 8/\sigma$. (The constant in $\ll$ depends on n and σ .)

We note that the value of $c(1, 3)$ given in [4] is $\frac{8}{3}$, and so our result is an improvement on the size of n for $\sigma < \frac{1}{3}$. Also we wish to point out that the exponent $\frac{1}{3} + \sigma$ is certainly not the best possible value for a small solution of a cubic congruence. Indeed, in [2], Schmidt shows that for any $\varepsilon > 0$ there exists an $n_0 = n_0(r, d, \varepsilon)$ such that for $n > n_0$ (1) has a nonzero solution $\mathbf{x}$ with $|\mathbf{x}| \ll p^\varepsilon$.

In [1], Davenport and Lewis introduced the concept of the h -invariant of a cubic form. Specifically, for a cubic form $C(\mathbf{x})$ over $\mathbf{F}_p$, the h -invariant $h = h_p(C)$ (relative to the field $\mathbf{F}_p$) is the smallest positive integer h such that $C(\mathbf{x})$ can be written in the form

$$C(\mathbf{x}) = L_1(\mathbf{x})Q_1(\mathbf{x}) + L_2(\mathbf{x})Q_2(\mathbf{x}) + \dots + L_h(\mathbf{x})Q_h(\mathbf{x})$$

Received by the editors June 30, 1988, and, in revised form, September 25, 1988.

1980 *Mathematics Subject Classification* (1985 Revision). Primary 11D79; Secondary 11L40.

©1989 American Mathematical Society
0002-9939/89 \$1.00 + \$.25 per page

where $L_1, \dots, L_h$ are linear forms and $Q_1, \dots, Q_h$ are quadratic forms over $\mathbb{F}_p$. Thus $n - h_p(C)$ is the largest dimension of any subspace of $\mathbb{F}_p^n$ on which $C(\mathbf{x})$ is identically zero. Davenport and Lewis used the h -invariant to bound complete exponential sums. Schmidt [3] later extended the definition of an h -invariant to an arbitrary system of forms and was able to bound both complete and incomplete exponential sums in terms of h . We need the following Lemma, which is a special case of Theorem 3 of [3].

Lemma. *The congruence $C(\mathbf{x}) \equiv 0 \pmod{p}$ has a nonzero solution $\mathbf{x}$ with $|\mathbf{x}| \ll p^{1/3+\sigma}$ provided that $h_p(C) > 8/3\sigma$.*

Proof. Let $h = h_p(C)$. Suppose first that $h \leq n/3 + n\sigma$. Then $C(\mathbf{x})$ vanishes on an $n - h$ dimensional subspace of $\mathbb{F}_p^n$ and this subspace corresponds with a lattice of points in $\mathbb{Z}^n$ of volume p^h on which $C(\mathbf{x}) \equiv 0 \pmod{p}$. Thus, by Minkowski's fundamental theorem from the geometry of numbers, there exists a nonzero point $\mathbf{x}$ with $|\mathbf{x}| \leq p^{h/n} \leq p^{1/3+\sigma}$ and $C(\mathbf{x}) \equiv 0 \pmod{p}$.

If $h > n/3 + n\sigma$ then the theorem follows from the Lemma and our assumption that $n > 8/\sigma$.

REFERENCES

1. H. Davenport and D. J. Lewis, *Exponential sums in many variables*, Amer. J. Math. **84** (1962), 649–665.
2. W. M. Schmidt, *Diophantine inequalities for forms of odd degree*, Advances in Math. **38** (1980), 128–151.
3. —, *Bounds for exponential sums*, Acta Arithmetica **44** (1984), 281–297.
4. —, *Small solutions of congruences with prime modulus*, Diophantine analysis, Proc. Number Theory Sect. Aust. Math. Soc. Conv. 1985, London Math. Soc. Lect. Note Ser. **109** (1986), 37–66.

MATHEMATICS DEPARTMENT, KANSAS STATE UNIVERSITY, MANHATTAN, KANSAS 66506