SMALL SOLUTIONS OF CUBIC CONGRUENCES

TODD COCHRANE

(Communicated by William W. Adams)

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

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

$$F_1(x) = F_2(x) = \cdots = F_r(x) = 0 \pmod{p}$$

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

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 $\sigma < \frac{8}{3}$. 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 $\epsilon > 0$ there exists an $n_0 = n_0(r, d, \epsilon)$ such that for $n > n_0$ (1) has a nonzero solution $x$ with $|x| \ll p^\epsilon$.

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

$$C(x) = L_1(x)Q_1(x) + L_2(x)Q_2(x) + \cdots + L_h(x)Q_h(x)$$

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

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
where $L_1, \ldots, L_h$ are linear forms and $Q_1, \ldots, Q_h$ 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 $C(x)$ 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 $C(x) \equiv 0 \pmod{p}$ has a nonzero solution $x$ with $|x| \ll p^{1/3+\sigma}$ provided that $h_p(C) > 8/3\sigma$.

**Proof.** Let $h = h_p(C)$. Suppose first that $h \leq n/3 + n\sigma$. Then $C(x)$ 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 $C(x) \equiv 0 \pmod{p}$. Thus, by Minkowski’s fundamental theorem from the geometry of numbers, there exists a nonzero point $x$ with $|x| \leq p^{h/n} \leq p^{1/3+\sigma}$ and $C(x) \equiv 0 \pmod{p}$.

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

**References**


*Mathematics Department, Kansas State University, Manhattan, Kansas 66506*