ILLINOIS JOURNAL OF MATHEMATICS
Volume 31, Number 4, Winter 1987

SMALL SOLUTIONS OF CONGRUENCES OVER ALGEBRAIC NUMBER FIELDS

BY

TODD COCHRANE

1. Introduction

Let R be the ring of integers in a number field K, A be a nonzero ideal in R and $f_1(\mathbf{x}), \ldots, f_k(\mathbf{x})$ be homogeneous polynomials in n variables over R. In this paper we obtain small solutions to the system of congruences

$$f_1(\mathbf{x}) \equiv \cdots \equiv f_k(\mathbf{x}) \equiv 0 \pmod{A}, \tag{1.1}$$

the notion of smallness being given two interpretations, as indicated in Lemma 2.

The problem of finding small solutions of congruences has received considerable attention in the case where R is the set of rational integers. For instance, Schinzel, Schlickewei and Schmidt [6, Theorem 1] have shown that for any positive integer m and quadratic form $Q(\mathbf{x})$ over $\mathbf{Z}$ in $n \geq 3$ variables, there is a nonzero solution $\mathbf{x}$ of the congruence

$$Q(\mathbf{x}) \equiv 0 \pmod{m} \tag{1.2}$$

such that $\max|x_i| < m^{1/2+1/2(n-1)}$. Using the same method of proof, Heath-Brown [4, Theorem 2] has shown that if $n = 4$, m is an odd prime and $\det Q$ is a square (mod m), then (1.2) has a nonzero solution with $\max|x_i| < m^{1/2}$.

In this paper we generalize the geometric method of Schinzel et al [6] to algebraic number fields and apply it in turn to systems of linear forms, quadratic forms and forms of higher degree.

We wish to thank our thesis advisor Donald J. Lewis under whom most of this work was conducted, and Hugh L. Montgomery for his comments on the writing of this paper. We also wish to thank Wolfgang M. Schmidt for helping us detect the limitations of this method for forms of degree > 2.

Received February 3, 1986.

2. A lemma

We begin by proving the following result.

LEMMA 1. *Let* $\mathbf{F}(\mathbf{x})$ *be a k-tuple of forms in* $R[x_1, \ldots, x_n]$ *and* A *a nonzero ideal in* R *written as* $A = BC^2$ *where* $B = \prod_{i=1}^{s} P_i$, *a product of distinct prime ideals. Suppose that for* $i = 1, \ldots, s$ *there exists a subspace of* $[R/P_i]^n$ *of dimension* d_i, *(as an* R/P_i *vector space), on which* $\mathbf{F}(\mathbf{x}) \equiv \mathbf{0} \pmod{P_i}$. *Then:*

(a) *There exists an R-submodule* L *of* R^n *on which* $\mathbf{F}(\mathbf{x}) \equiv \mathbf{0} \pmod{B}$, *such that*

$$[R^n: L] = \prod_{i=1}^{s} |R/P_i|^{n-d_i}.$$

(b) *If all of the* f_i *have degrees* ≥ 2, *then there exists an R-submodule* M *of* R^n *on which* $\mathbf{F}(\mathbf{x}) \equiv \mathbf{0} \pmod{A}$ *such that* $[R^n: M] = |R/C|^n \prod_{i=1}^{s} |R/P_i|^{n-d_i}$.

Proof. For $i = 1, \ldots, s$ let V_i be the subspace of $[R/P_i]^n$ of dimension d_i on which $\mathbf{F}$ vanishes. The inverse image of $V_1 \times V_2 \times \cdots \times V_s$ in R^n under the mapping

$$R^n \twoheadrightarrow [R/B]^n \xrightarrow{\sim} [R/P_1]^n \times \cdots \times [R/P_s]^n,$$

is an R-submodule L of R^n satisfying the conditions of part(a).

Now suppose that all of the f_i have degrees ≥ 2. Let M be the submodule of R^n given by

$$M = CL = \left\{ \sum_{i=1}^{t} c_i \mathbf{y}_i \colon c_i \in C, \mathbf{y}_i \in L, t > 0 \right\}.$$

Since R/A is a principal ideal ring it follows that every point in M satisfies the congruence $\mathbf{F}(\mathbf{x}) \equiv \mathbf{0} \pmod{A}$. Moreover $|R^n/CL| = |R/C|^n |R^n/L|$, finishing the proof.

3. Small solutions in number fields

Let K be a number field of degree m over $\mathbf{Q}$, d the discriminant of K over $\mathbf{Q}$, R the ring of integers in K, and say $m = r + 2s$ where r is the number of real conjugates of K and $2s$ is the number of complex conjugates. For any $x \in K$ let $N(x) = N_{K/\mathbf{Q}}(x)$ denote the norm of x, and $\|x\|$ denote the size of x, that is, the maximum of the absolute values of the conjugates of x. For any nonzero ideal A in R, let $N(A) = |R/A|$ denote the absolute norm of A. We

can define the notion of smallness in various ways, two of which are treated in the following

LEMMA 2. *Let M be an additive subgroup of R^n of finite index.*

(a) *There exists a nonzero point $\mathbf{x} = (x_1, \ldots, x_n)$ in M such that*

$$\max|N(x_i)| \leq \alpha_K[R^n: M]^{1/n} \quad \text{where } \alpha_K = \frac{m!}{m^m}\left(\frac{4}{\pi}\right)^s |d|^{1/2}.$$

(b) *There is a nonzero point $\mathbf{y} = (y_1, \ldots, y_n)$ in M such that*

$$\max\|y_i\| \leq \left(\left(\frac{2}{\pi}\right)^s d^{1/2}[R^n: M]^{1/n}\right)^{1/m}.$$

Proof. To prove parts (a) and (b) we use the canonical imbedding of R^n into $\mathbf{R}^{mn}$ defined as follows. For any x in R let

$$\sigma(x) = (x^{(1)}, \ldots, x^{(r)}, \operatorname{Re} x^{(r+1)}, \operatorname{Im} x^{(r+1)}, \ldots, \operatorname{Re} x^{(r+s)}, \operatorname{Im} x^{(r+s)})$$

where $x^{(1)}, \ldots, x^{(r)}$ are the real conjugates of x and $x^{(r+1)}, \ldots, x^{(r+s)}$, $\bar{x}^{(r+1)}, \ldots, \bar{x}^{(r+s)}$ are the complex conjugates of x. Define $\hat{\sigma}\colon R^n \to \mathbf{R}^{mn}$ by

$$\hat{\sigma}(x_1, \ldots, x_n) = (\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_n)).$$

Then $\hat{\sigma}(R^n)$ is a lattice in $\mathbf{R}^{mn}$ of volume $2^{-sn}d^{n/2}$ (For example, see [5, p. 56]), and $\hat{\sigma}(M)$ is a sublattice $\mathscr{L}$ of $\hat{\sigma}(R^n)$ of volume $[R^n: M]2^{-sn}d^{n/2}$. (By volume of a lattice we mean the volume of a fundamental parallelepiped.)

For any positive number λ, let $S_1(\lambda)$ be the set of mn-tuples

$$(x_{11}, \ldots, x_{1m}, x_{21}, \ldots, x_{2m}, \ldots, x_{n1}, \ldots, x_{nm})$$

in R^{mn} satisfying the inequalities

$$|x_{i1}| \cdots |x_{ir}||x_{ir+1}^2 + x_{ir+2}^2| \cdots |x_{im-1}^2 + x_{im}^2| \leq \lambda, \quad 1 \leq i \leq n.$$

By the inequality of the arithmetic and geometric means, $S_1(\lambda)$ contains the convex body $S_2(\lambda)$ defined by the inequalities

$$|x_{i1}| + \cdots + |x_{ir}| + 2|x_{ir+1}^2 + x_{ir+2}^2|^{1/2} + \cdots + 2|x_{im-1}^2 + x_{im}^2|^{1/2} \leq m\lambda^{1/m},$$

$i = 1, \ldots, n$. It is well known that the volume of $S_2(\lambda)$ is $(\lambda 2^{r-s}m^m\pi^s/m!)^n$, (e.g., see [5, p. 66]), and thus by Minkowski's fundamental theorem, $S_2(\lambda)$ contains a nonzero point $\mathbf{p}$ of $\mathscr{L}$ if $\lambda = \alpha_K[R^n: M]^{1/n}$. It is clear that $\hat{\sigma}^{-1}(\mathbf{p})$ is a nonzero point of M all of whose components have norms bounded by λ.

To prove (b) we proceed as above replacing the region $S_1(\lambda)$ by the convex body $S_3(\lambda)$ defined by

$$|x_{ij}| \leq \lambda, \quad 1 \leq i \leq n, 1 \leq j \leq r,$$

$$|x_{ij}^2 + x_{ij+1}^2| \leq \lambda^2, \quad i = 1, \ldots, n, \; j = r+1, r+3, \ldots, m-1.$$

The volume of $S_3(\lambda)$ is $(2^r \lambda^r \pi^s \lambda^{2s})^n$ and so now it suffices to take

$$\lambda = \left(\left(\frac{2}{\pi} \right)^s d^{1/2} [R^n : M]^{1/n} \right)^{1/m}.$$

4. Linear congruences

Let $U = [u_{ij}]$ be a $k \times n$ matrix over $\mathbf{Z}$ of rank r. For any positive integer m let $\ker_m(U)$ denote the set of points in $[\mathbf{Z}/(m)]^n$ satisfying the linear system of congruences $U\mathbf{x}^T \equiv \mathbf{0}^T \pmod m$, where $\mathbf{x}^T$ is a column matrix of variables $x_1, \ldots, x_n$, and $\mathbf{0}^T$ is a column matrix of zeros. Since $\mathbf{Z}$ is a P.I.D. there exist matrices $S \in M_k(\mathbf{Z})$ and $T \in M_n(\mathbf{Z})$, with $\det S = \pm 1$, $\det T = \pm 1$ such that SUT is a diagonal matrix with diagonal entries $(d_1, \ldots, d_r, 0, \ldots, 0)$, where $d_1, \ldots, d_r$ are the invariant factors of U.

It is clear that $\mathbf{x} \in \ker_m(\mathrm{SUT})$ if and only if $x_i \equiv 0 \pmod{m/(m, d_i)}$, $i = 1, \ldots, r$. Thus, since $\ker_m U \simeq \ker_m \mathrm{SUT}$ we have

$$|\ker_m U| = \left[\prod_{i=1}^{r} (m, d_i) \right] m^{n-r}.$$

Let M be the set of points in $\mathbf{Z}^n$ satisfying $U\mathbf{x}^T \equiv \mathbf{y}^T \pmod m$; it follows that

$$[\mathbf{Z}^n : M] = m^r \Big/ \prod_{i=1}^{r} (m, d_i)$$

and hence by Lemma 2 we deduce:

THEOREM 1. *For any positive integer m and $k \times n$ matrix U over $\mathbf{Z}$ with invariant factors $d_1, \ldots, d_r$ there is a nonzero solution $\mathbf{x}$ of the congruence $U\mathbf{x}^T \equiv \mathbf{0}^T \pmod m$ such that*

$$\max |x_i| \leq m^{r/n} \Big/ \prod_{i=1}^{r} (m, d_i)^{1/n}.$$

This improves Theorem 1 of A. Brauer and R. L. Reynolds [3] who made use of the pigeon-hole principle to obtain a solution with $0 < \max|x_i| \leq m^{k/n}$. We note in particular that the bound given in Theorem 1 is nontrivial if $(d_r, m) > 1$, even when $r = k = n$. It is easy to construct examples showing that the exponent r/n in Theorem 1 is best possible. For example the congruence

$$x_1 + bx_2 + b^2x_3 + \cdots + b^{n-1}x_n \equiv 0 \pmod{m}, \tag{4.1}$$

where $b = [m^{1/n}]$, has no nonzero solution with $\max|x_i| < [m^{1/n}]$. A second example is

$$\begin{aligned} x_2 &\equiv bx_1 \pmod{m} \\ x_3 &\equiv b^2x_1 \pmod{m} \\ &\vdots \\ x_n &\equiv b^{n-1}x_1 \pmod{m}. \end{aligned} \tag{4.2}$$

One can easily show that there is no nonzero solution of (4.2) with $\max|x_i| < b^n/(b+1)$. Thus for any $\varepsilon > 0$ there is a positive number $m_0(\varepsilon)$ such that if $m > m_0(\epsilon)$ then (4.2) has no nonzero solution with $\max|x_i| < (1-\epsilon)m^{(n-1)/n}$.

More generally, for any k and n with $k < n$ and any prime p, we can show that there exists a $k \times n$ system of congruences (mod p) such that $\max|x_i| \geq \frac{1}{2}[p^{k/n}]$ for all nonzero solutions $\mathbf{x}$. Indeed, any integral point $\mathbf{x}$, with $\mathbf{x} \not\equiv \mathbf{0} \pmod{p}$ is a solution of $p^{(n-1)k}$ distinct $k \times n$ systems (mod p). Thus for any set S of distinct nonzero integral points (mod p) such that $p^{nk} > |S|p^{(n-1)k}$, there exists some $k \times n$ system having no solution in S.

For a general Dedekind domain one can prove the following analogue of Theorem 1, albeit a weaker version.

PROPOSITION 1. *Let U be a $k \times n$ matrix over a Dedekind domain R, of rank r over the field of fractions of R. Let A be a nonzero ideal in R and M the set of points in R^n satisfying the congruence $U\mathbf{x}^T \equiv \mathbf{0}^T \pmod{A}$. Then $[R^n: M] \leq |R/A|^r$.*

In particular, if R is the ring of integers in a number field K, then there is a nonzero solution $\mathbf{x}$ of the congruence $U\mathbf{x}^T \equiv \mathbf{0}^T \pmod{A}$ such that $\max|N(x_i)| \leq \alpha_K|N(A)|^{r/n}$, α_K as given in Lemma 2.

5. Systems of quadratic forms

LEMMA 3. *Let $Q_1(\mathbf{x}), \ldots, Q_k(\mathbf{x})$ be quadratic forms in n variables over a finite field F_q.*

(a) *For* $1 \le k < n/2$ *there exists a subspace of* F_q^n *of dimension* $[(n - k)/(k + 1)]$ *on which* $Q_1, \ldots, Q_k$ *are identically zero. (This holds even when q is even.)*

(b) *If q is odd, n is even and* $Q(\mathbf{x})$ *is a quadratic form of determinant* Δ, *then* $Q(\mathbf{x})$ *vanishes on an* $n/2$ *dimensional subspace if and only if* $(-1)^{n/2}\Delta$ *is a square in* F_q.

(c) *If q is odd, then any two quadratic forms* Q_1, Q_2 *vanish on a subspace of dimension* $[(n - 3)/2]$.

David Leep has informed me that he can prove (c) when q is even as well.

Proof. Part (a) can be proved by induction on the dimension of the subspace, using Chevalleys's Theorem. Part (b) follows from the fact that the dimension of any maximal isotropic subspace of the quadratic space (F_q^n, Q) is $\frac{1}{2}$ the dimension of the hyperbolic part of F_q^n relative to Q.

Part (c) follows readily from a theorem of Amer [1, Satz 8] which states that for any field F of characteristic $\neq 2$, any two quadratic forms Q_1, Q_2 over F have a d-dimensional subspace of common zeros if and only if $Q_1 + tQ_2$ has a d-dimensional subspace of zeros over $F(t)$, where t is an indeterminate. But any quadratic form in 5 variables over $F_q(t)$ has a nontrivial zero in $F_q(t)$ and so it follows that $Q_1 + tQ_2$ has a $[(n - 3)/2]$ dimensional subspace of zeros.

THEOREM 2. *Let* $Q_1, \ldots, Q_k$ *be quadratic forms in n variables over the ring of integers R in a number field K, and let A be a nonzero ideal in R. Suppose that* $k < n/2$. *Then there exists a nonzero solution* $\mathbf{x} \in R^n$ *of the congruences*

$$Q_1(\mathbf{x}) \equiv \cdots \equiv Q_k(\mathbf{x}) \equiv 0 \pmod{A} \tag{5.1}$$

such that

$$\max|N(x_i)| \le \alpha_K |N(A)|^{k/(k+1)+k/(k+1)(n-l)} \tag{5.2}$$

where l is the remainder upon dividing $(n - k)$ *by* $(k + 1)$.

Remarks. An analogous statement can be made for the other type of "smallness" discussed in Lemma 2. Also, parts (b) and (c) of Lemma 3 give rise to sharper versions of the theorem when $k = 1$ or 2. When $k = 2$ we obtain $\max|N(x_i)| \le \alpha_K |N(A)|^{1/2+3/2(n-1)}$.

Proof. First assume that $(k + 1)|(n - k)$. Let $A = BC^2$, $B = \prod_{i=1}^{s} P_i$. For $i = 1, \ldots, s$ there exists a subspace of $[R/P_i]^n$ of dimension $(n - k)/(k + 1)$ on which $Q_1, \ldots, Q_k$ are identically zero. Thus by Lemma 1 there is an R-module M of solutions of (5.1) such that

$$\begin{aligned}[R^n\colon M] &= |N(C)|^n \prod_{i=1}^{s} |N(P_i)|^{n-(n-k)/(k+1)} \\ &\le |N(A)|^{k(n+1)/(k+1)}.\end{aligned}$$

By Lemma 2, M contains a nonzero point $\mathbf{x}$ such that $\max|N(x_i)|$ satisfies (5.2). If $(k+1) \nmid (n-k)$ then we set l variables equal to zero from the start, where l is the remainder upon dividing $(n-k)$ by $(k+1)$.

When $K = \mathbf{Q}$ and $k = 1$ then Theorem 2 is just Theorem 1 of Schinzel, Schlickewei and Schmidt [6]. For a system of k quadratic forms over $\mathbf{Z}$ and any positive integer m, R. Baker [2, Theorem 1] has shown that for any $\epsilon > 0$, if $n > n_0(\epsilon, k)$ then there is a solution of

$$Q_1(\mathbf{x}) \equiv \cdots \equiv Q_k(\mathbf{x}) \equiv 0 \pmod{m}$$

such that $0 < \max|x_i| < m^{(1/2)+\epsilon}$. However, no estimate was given on how large n must be. If the number of variables is relatively small compared to k, then one cannot expect to do better than a size of $m^{k/(k+1)}$ as the following example shows.

Example. Let $n = 2(k+1)$, p be a prime, α be a quadratic nonresidue (mod p) and

$$L_i(\mathbf{x}) = L_i(x_1, \ldots, x_{k+1}), \quad 1 \le i \le k,$$

be a system of linear forms as given by (4.2). For $i = 1, \ldots, k$ set

$$Q_i(x_1, \ldots, x_n) = L_i(x_1, \ldots, x_{k+1})^2 - \alpha L_i(x_{k+2}, \ldots, x_n)^2.$$

If $\mathbf{x}$ is a nonzero solution of $Q_1(\mathbf{x}) \equiv \cdots \equiv Q_k(\mathbf{x}) \equiv 0 \pmod{p}$ then

$$\max|x_i| \ge \left(\frac{b}{b+1}\right)\left[p^{1/(k+1)}\right]^k$$

where $b = [p^{1/(k+1)}]$. In this case, Theorem 2 gives us a nonzero solution with $\max|x_i| < p^{k/(k+1)+k/(k+1)(2k+1)}$. One would like to be able to remove the extra piece $k/(k+1)(2k+1)$ from the exponent.

6. Further discussion

The method of obtaining small solutions as in Lemma 1 breaks down when we apply it to forms of degree greater than two. The difficulty stems from the fact that if $d < q$ and $n < (1/d!)l^{d-1}$ then there exists a form of degree d over $\mathbf{F}_q$ in n variables which does not vanish on any l-dimensional subspace of $\mathbf{F}_q^n$, (as a counting argument will readily verify). Now, the effectiveness of Lemma 1 depends on the size of l/n: the larger this ratio, the smaller the solution we obtain. Thus for a single form of degree d with $2 < d < n$ the best

we can do is to set all but $d + 1$ variables equal to zero and settle for a one dimensional subspace of zeros of the resulting form. This idea yields:

PROPOSITION 2. *Let R be the ring of integers in a number field K, A a nonzero ideal in R and $f_1(\mathbf{x}), \ldots, f_k(\mathbf{x})$ forms in $R[x_1, \ldots, x_n]$. If $n > \delta = \sum_{i=1}^{k} \deg(f_i)$ then there exists a nonzero solution $\mathbf{x}$ of (1.1) such that*

$$\max|N(x_i)| \leq \alpha_K |N(A)|^{\delta/(\delta+1)}.$$

Remark. The restriction on n given in Proposition 2 cannot be weakened, for if $n = \sum_{i=1}^{k} \deg(f_i)$ then (1.1) may not have any nonzero solutions.

REFERENCES

1. M. AMER, *Quadratische formen über funktionenkörpern*, Dissertation, Mainz, 1976.
2. R.C. BAKER, *Small solutions of quadratic and quartic congruences*, Mathematika, vol. 27 (1980), pp. 30–45.
3. A. BRAUER and R.L. REYNOLDS, *On a theorem of Aubry-Thue*, Canad. J. Math., vol. 3 (1951), pp. 367–374.
4. D.R. HEATH-BROWN, *Small solutions of quadratic congruences*, to appear.
5. P. SAMUEL, *Algebraic theory of numbers*, Hermann, Paris, 1970.
6. A. SCHINZEL, H.P. SCHLICKEWEI and W.M. SCHMIDT, *Small solutions of quadratic congruences and small fractional parts of quadratic forms*, Acta Arithmetica, vol. 37 (1980), pp. 241–248.

KANSAS STATE UNIVERSITY
MANHATTAN, KANSAS