Small Solutions for System of Homogenous Polynomials Congruences over a Dedekind Domain

Ali H. Hakami

Department of Mathematics, Faculty of Science, Jazan University
P.O. Box 277, Jazan, Postal Code: 45142, Saudi Arabia

Abstract
Let \( f_1(x), \ldots, f_k(x) \) be homogeneous polynomials in \( n \) variables over the ring of integers \( R \) in a number field, and let \( A \) be a nonzero ideal in \( R \). In [1], Cochrane generalized the geometric idea of Schinzel, Schlickewei and Schmidt used it in [15] to obtain small solutions to the system of congruences \( f_1(x) \equiv \cdots \equiv f_k(x) \equiv 0 \pmod{A} \), the notation of a small point being given two interpretations, a point having coordinates with small norms, and a point having coordinates of small size. In this paper, we shall follow [1] and [15] to find small solutions of the above system over a Dedekind domain.

Mathematics Subject Classification: Primary 11C08, 11D79, 13F05, 13F20

Keywords: Homogenous polynomials, congruences, solutions, Dedekind domain

1 Introduction
Let \( R \) be the ring of integers in a number field \( K \), \( A \) be a nonzero ideal in \( R \) and \( f_1(x), \ldots, f_k(x) \) be homogeneous polynomials in \( n \) variables over \( R \). In this paper we obtain small solutions to the system of congruences
\[ f_1(x) \equiv f_2(x) \equiv \cdots \equiv f_k(x) \equiv 0 \pmod{A}, \tag{1.1} \]
the notion of smallness being given two interpretations, as indicated in Lemma 2.1. The problem of finding small solutions of congruences has received considerable attention in case where \( \mathbb{R} \) is the set of rational integers. For instance, Schinzel, Schlickewei and Schmidt [15] have shown that for any positive \( m \) and quadratic form \( Q(x) \) over \( \mathbb{Z} \) in \( n \geq 3 \) variables, there is a nonzero solution \( x \) of the congruence

\[
Q(x) = Q(x_1, x_2, \ldots, x_n) \equiv 0 \pmod{m} \quad (1.2)
\]
such that \( \max |x_i| < m^{\frac{1}{2} + \frac{1}{2(n-1)}} \). Using the same method of proof, Heath-Brown [13] has shown that if \( n = 4 \), \( m \) is an odd prime and \( \det Q \) is a square \( \pmod{m} \), then (1.2) has a nonzero solution with \( \max |x_i| \leq m^{1/2} \).

Dealing with \( m = p \), \( p \) an odd prime, Heath-Brown [14] obtained a nonzero solution of (2.1) with \( \max |x_i| < p^{1/2} \log p \) for \( n \geq 4 \). His result was an improvement on the result of [15] in this case. Wang Yuan [16, 17] and [18] generalized Heath-Brown’s work to all finite fields. Cochrane, in a sequence of papers [2], [3] and [5] improved this to \( \max |x_i| < \max \{2^{19}p^{1/2}, 2^{22}10^6\} \). The best constant available is due to Hakami [8] and [9] who obtained \( \max |x_i| < \min \{p^{2/3}, 2^{19}p^{1/2}\} \).

Using the method of exponential sums Hakami [10] generalized Cochrane’s method to find a nonzero solution of (2) with \( \max |x_i| < p \) for \( n \geq 4 \) when \( m = p^2 \) and \( Q(x) \) is nonsingular \( \pmod{p} \). The optimal bound, \( \max |x_i| < p \) for \( n \geq 1 \), was obtained by Cochrane and Hakami (using geometric method) [7].

For \( m = p^3 \), Hakami [11] obtained bound with \( \max |x_i| < p^{3\frac{3}{2} + \frac{3}{n}} \), provided \( n \geq 6 \).

For general power \( m = p^k \) and nonsingular form \( \pmod{p^k} \) in \( n \geq 4 \) variables (\( n \) even) a primitive solution of size \( \max |x_i| < \frac{1}{2} + \frac{3}{n} \) is obtained by the author [12].

For \( m = pq \) a product of two distinct primes, the optimal bound, \( \max |x_i| < m^{\frac{1}{2} + \varepsilon} \), for \( n > 4 \) was obtained by Cochrane [4] and [6], building upon the work of Heath-Brown [13].

In this paper, we follow Cochrane [1] and Schinzel, Schlickewei and Schmidt [15] to generalize the geometric idea which used in their work, to find small solutions of the system (1.1) over a general Dedekind domain.

2 Definitions and Lemmas

Let \( K \) be a number field of degree \( m \) over \( \mathbb{Q} \), \( d \) the discriminant \( K \) over \( \mathbb{Q} \), \( R \) 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 $N(x) = N_{K/Q}(x)$ denote the norm of $x$, and $\|x\|$ denote the size of $x$, that is the maximum of the absolute value 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 notation of smallness in various ways, three of which are treated in the following:

**Lemma 2.1** ([1], Theorem 3) Let $M$ be an additive subgroup of $R^n$ of finite index, then

a) There exists a nonzero point $x = (x_1, \ldots, x_n)$ in $M$ such that
$$\max |N(x_i)| \leq \alpha_K [R^n : M]^{1/n},$$
where $\alpha_K$ is a constant depending only on $K$, $\alpha_K = \frac{m!}{m^m} (\frac{4}{\pi})^s |d|^{1/2}$.

b) There is a nonzero point $y = (y_1, \ldots, y_n)$ in $M$ such that
$$\max \|y_i\| \leq (\frac{2}{\pi})^s |d|^{1/2} [R^n : M]^{1/n} 1/m.$$  

c) If $w_1, \ldots, w_m$ is an integral basis for $R$ over $\mathbb{Z}$ then there is a nonzero point $z = (z_1, \ldots, z_n)$ in $M$, $z_i = \sum_{j=1}^{m} z_{ij}w_j$, such that
$$|z_{ij}| \leq [R^n : M]^{1/mn}, \quad 1 \leq i \leq n, 1 \leq j \leq m.$$  

3 The Main Results

Let $R$ be a Dedekind domain having the property that $R/P$ is a finite field for any prime ideal $P$ in $R$. Let $U = (u_{ij})$ be a $k \times n$ matrix, $k \leq n$, with entries in $R$ and let $r = r(U)$ denote the rank of $U$ as a matrix over the field of fractions of $R$. For any nonzero ideal $A$ in $R$, let $\ker_A(U)$ be the set of points in $[R/A]^n$ satisfying
$$UX^T \equiv 0^T \pmod A. \quad (3.1)$$

**Theorem 3.1** Let $M$ be the set of points in $R^n$ satisfying (3.1), then $M$ is an $R$-submodule of $R^n$ of index
$$[R^n : M] \leq |R/A|^r.$$  

Using Lemma 2.1 (a) we obtain the following corollary which follow directly from Theorem 3.1.

**Corollary 3.2** If $R$ is the ring of integers in a number field $K$, then there is a nonzero solution of (3.1) such that
$$\max |N(x_i)| \leq \alpha_K |N(A)|^{r(U)/n}, \quad 1 \leq i \leq n,$$
where $\alpha_K$ is as given in Lemma 1.2 (a).
4 Proof of Theorem 3.1

First we claim there exist matrices $S \in M_k(R)$ and $T \in M_n(R)$ such that $\det S$ and $\det T$ are both relatively prime to $A$, and

$$SUT \equiv \begin{pmatrix} d_1 & 0 \\ d_2 & \ddots \\ 0 & \ddots & \ddots \\ \end{pmatrix} \pmod{A}, \quad \text{(4.1)}$$

for some $d_1, ..., d_r$ in $R$. To prove this, we first assume $A = P^e$, a power of a prime ideal. We can view $ar{U}$ as a matrix with entries in $R_P$, $(R$ localized at $P$.) Since $R_P$ is a principal ideal domain, there exist matrices $S' \in M_k(R_P)$ and $T' \in M_n(R_P)$ such that $\det S'$ and $\det T'$ are units in $R_P$ and

$$S'UT' = \begin{pmatrix} d'_1 & 0 \\ d'_2 & \ddots \\ 0 & \ddots & \ddots \\ \end{pmatrix} = D',$$

for some $d'_1, ..., d'_r$ in $R_P$, we have

$$S'UT' \equiv D' \pmod{P^e}.$$

But

$$R/P^e \simeq R_P/P^e R_P,$$

so that there exist matrices $S \in M_k(R)$ and $T \in M_n(R)$ such that $\det S$ and $\det T$ are relatively prime to $P$, and

$$SUT \equiv \begin{pmatrix} d_1 & 0 \\ d_2 & \ddots \\ 0 & \ddots & \ddots \\ \end{pmatrix} \pmod{P^e},$$

for some $d_1, ..., d_r$ in $R_P$.

Now suppose that $A = \prod_{i=1}^s P_i^{e_i}$. For $i = 1, ..., s$ we can find $S_i \in M_k(R)$,
Solutions for system of congruence over a Dedekind domain

345

$T_i \in M_n(R)$ such that $\det S_i$ and $\det T_i$ are relatively prime to $P_i$, and

$$S_iUT_i \equiv \begin{pmatrix} d_{1i} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & d_{ri} \end{pmatrix} \pmod{P_i^{e_i}},$$

for some $d_{ji} \in R$, $1 \leq j \leq r$. By the CRT we can find matrices $S \in M_k(R)$ and $T \in M_n(R)$ such that

$$S \equiv S_i \pmod{P_i^{e_i}} \quad \text{and} \quad T \equiv T_i \pmod{P_i^{e_i}}, \quad 1 \leq i \leq s,$$

that is, all of the corresponding entries are congruent $(\pmod{P_i^{e_i}})$. It is clear that $SUT$ is a diagonal-type matrix $(\pmod A)$ as given in (4.1). Moreover, since

$$\det S \equiv \det S_i \pmod{P_i^{e_i}}, \quad 1 \leq i \leq s,$$

it is also clear that $\det S$ is relatively prime to $A$ and and likewise $\det T$ is relatively prime to $A$. (In fact, the $d_i$ in (4.1) can be arranged so that $\nu_P(d_i) \leq \nu_P(d_{i+1})$ for all primes $P | A$, where $\nu_P$ is the valuation on $R$ corresponding to $P$). Since the matrices $S$ and $T$ have inverses when viewed over the ring $R/A$, we have

$$\ker_A(U) = \ker_A(SU) \simeq \ker_A(SUT) \quad (\text{as } R\text{-modules}).$$

It is clear that $\ker_A(SUT)$ contains the set

$$\{y = (y_1, \ldots, y_n) \in [R/A]^n : y_1 \equiv y_2 \equiv \cdots \equiv y_r \equiv 0 \pmod{A}\},$$

so that $|\ker_A(SUT)| \geq |R/A|^{n-r}$. Hence

$$[R^n : M] = [[R/A]^n : \ker_A(U)] \leq |R/A|^r.$$

5 Remarks

1) We observe that Corollary 3.1 is an analogue of Lemma 2.1 (a), but a little bet a weaker version.

2) Analogous statements can be made for the other types of smallness mentioned in Lemma 2.1.

Acknowledgements. The author would like to thank Professor Ibrahim Saleh, University of Wisconsin, USA, for his helpful comments and constructive suggestions. He is thankful to Jazan University (JU), Jazan, Saudi Arabia for providing excellent research facilities to carry out this research.
References


Solutions for system of congruence over a Dedekind domain


Received: September 12, 2015; Published: October 10, 2015