ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 26, Number 3, Summer 1996

SMALL SOLUTIONS TO SYSTEMS OF LINEAR CONGRUENCES OVER NUMBER FIELDS

EDWARD B. BURGER

Dedicated to Professor Wolfgang M. Schmidt on his 60th birthday

1. Introduction. There has been much activity, in recent years, in developing theorems from the classical geometry of numbers into the adèle space of a number field. The pioneering work in this area was done independently by McFeat [**11**] and Bombieri and Vaaler [**3**], who produced the adelic analogue of Minkowski's successive minima theorem. Such machinery has primarily been used to solve various diophantine problems. The adèle space approach has been amply justified by relatively simple inequalities, and a much clearer presentation of the roles played by arithmetic and the geometry of Euclidean space. In fact, arithmetic is the result of geometry at the nonarchimedean completions of the number field. Here we wish to illustrate these methods by producing new sharp upper bounds for the size of solutions to systems of linear congruences over number fields. In the early 1900's, Aubry [**1**] and Thue [**13**] independently proved the following result which is now often referred to as the Aubry-Thue theorem.

Theorem 1. *Let a, b and $m > 0$ be integers. Then there exists an integer solution to*

$$ax + by \equiv 0 \pmod{m}$$

where $0 < \max\{|x|, |y|\} \leq m^{1/2}$.

Improvements and generalizations in various directions were given by Vinogradov [**14**], De Backer [**9**], Ballieu [**2**] and Nagell [**12**]. In 1951 Brauer and Reynolds [**4**] used Dirichlet's box principle to prove the following extension of the Aubry-Thue theorem.

Theorem 2. *Let A be an $M \times N$ matrix having rational integer*

Received by the editors on October 26, 1994, and in revised form on April 25, 1995.

entries and $\operatorname{rank}(A) = M < N$ *and* $m > 0$ *an integer. Then there exists a (column) vector* $\mathbf{x} \in \mathbf{Z}^N$ *such that*

$$A\mathbf{x} \equiv \mathbf{0} \pmod{m} \quad \textit{and} \quad 0 < |\mathbf{x}| \leq m^{M/N},$$

where $\mathbf{x} = (x_1 x_2 \cdots x_N)^T$ *and* $|\mathbf{x}| = \max_{1 \leq n \leq N}\{|x_n|\}$.

Brauer and Reynolds also formulated a number field analogue in the case of one linear form in two variables, thus generalizing Theorem 1.

In 1987 Cochrane [**8**] improved the Brauer-Reynolds bound on $|\mathbf{x}|$ by replacing the box principle with Minkowski's convex body theorem. In particular, he proved

Theorem 3. *Let* A *be an* $M \times N$ *matrix having rational integer entries and* $\operatorname{rank}(A) = M < N$ *and* $m > 0$ *an integer. Then there exists a vector* $\mathbf{x} \in \mathbf{Z}^N$ *such that*

$$A\mathbf{x} \equiv \mathbf{0} \pmod{m} \quad \textit{and} \quad 0 < |\mathbf{x}| \leq m^{M/N} \prod_{i=1}^{M} \gcd(m, d_i)^{-1/N} \ ,$$

where $d_1, d_2, \ldots, d_M$ *are the invariant factors associated with* A.

Using the classical geometry of numbers over Euclidean N-space, Cochrane then produced a number field analogue that generalized the upper bound of Theorem 2. We remark that if the number field has class-number greater than one, then the ring of integers is not a unique factorization domain and hence greatest common divisors and invariant factors are no longer well-defined. Thus one cannot expect an improvement of Theorem 2 in this general setting to be of the form of Theorem 3.

Returning to the classical situation, if we let

$$\Lambda = \left\{\mathbf{x} \in \mathbf{Z}^N : A\mathbf{x} \in (m\mathbf{Z})^M\right\},$$

then Λ is easily seen to be a $\mathbf{Z}$-module of rank N in $\mathbf{R}^N$, that is, Λ is a *lattice* in $\mathbf{R}^N$. Thus it is natural to ask for N linearly independent vectors in Λ that are relatively small. Here we address this question and

prove a very general result over arbitrary number fields which we will show to be sharp. As a corollary we provide a number field analogue of Cochrane's improved upper bound where we replace the product of greatest common divisors of the invariant factors and the modulus with a product of local heights. In Section 4 we show that in the case when the number field is $\mathbf{Q}$ this upper bound is identical to that occurring in Theorem 3.

In Section 2 we carefully define all notation, but briefly, let k be an algebraic number field of degree d over $\mathbf{Q}$ with ring of integers $\mathcal{O}_k$. Let $\mathcal{I}$ be a fractional ideal in k. It follows that $\mathcal{I}$ may be factored uniquely into prime ideals in $\mathcal{O}_k$ as

$$\mathcal{I} = \prod_{v \nmid \infty} \mathcal{P}_v{}^{\mathfrak{e}_v},$$

where $\mathfrak{e}_v \in \mathbf{Z}$ with $\mathfrak{e}_v = 0$ for almost all places v of k. The sequence of exponents $\{\mathfrak{e}_v\}_{v \nmid \infty}$ is known as the *divisor* of $\mathcal{I}$. It follows that there is a natural one-to-one correspondence between divisors and fractional ideals. For each nonarchimedean place v of k, let π_v be a generator for the unique maximal ideal in the ring of v-adic integers $\mathcal{O}_v$. Given an $M \times N$ matrix A over k and fractional ideals $\mathcal{I}$ and $\mathcal{J}$ in k having divisors $\{\mathfrak{e}_v\}_{v \nmid \infty}$ and $\{\mathfrak{f}_v\}_{v \nmid \infty}$, respectively, we define an associated augmented $(M+N) \times N$ matrix $\mathcal{A}_v = \mathcal{A}_v(A, \mathcal{I}, \mathcal{J})$ over k_v by

$$\mathcal{A}_v = \begin{pmatrix} \pi_v^{-\mathfrak{e}_v} A \\ - \ - \ - \\ \pi_v^{-\mathfrak{f}_v} \mathbf{1}_N \end{pmatrix},$$

where $\mathbf{1}_N$ denotes the $N \times N$ identity matrix. Let c_k be the field constant defined in Section 2 by (2.1) and $H_v(\mathcal{A}_v)$ the normalized local height on the Grassmann coordinates of $\mathcal{A}_v$ also defined in Section 2. Finally we denote the N-fold Cartesian product of the fractional ideal $\mathcal{I}$ by $(\mathcal{I})^N$. Our main result is the following

Theorem 4. *Let A be an $M \times N$ matrix over k of $\operatorname{rank}(A) = M < N$. If $\mathcal{I}$ and $\mathcal{J}$ are fractional ideals in k and $\mathcal{A}_v = \mathcal{A}_v(A, \mathcal{I}, \mathcal{J})$ the associated $(M+N) \times N$ matrix over k_v for each nonarchimedean place v, then there exist N linearly independent vectors $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_N$ in k^N so that*

(i) $\mathbf{x}_n \in (\mathcal{J})^N$ *for all* $n = 1, 2, \ldots, N$.

(ii) $A\mathbf{x}_n \in (\mathcal{I})^M$ *for all* $n = 1, 2, \ldots, N$.

(iii)
$$\prod_{n=1}^{N} \prod_{v|\infty} |\mathbf{x}_n|_v \leq c_k^N \prod_{v\nmid\infty} H_v(\mathcal{A}_v) \ .$$

If the matrix A is over $\mathcal{O}_k$ and $\mathcal{I}$ is a nonzero ideal in $\mathcal{O}_k$, then by setting $\mathcal{J} = \mathcal{O}_k$, Theorem 4 provides the following number field analogue of the Cochrane formulation of the Aubry-Thue theorem.

Corollary 5. *Let A be an $M \times N$ matrix over $\mathcal{O}_k$ with* $\operatorname{rank}(A) = M < N$. *If $\mathcal{I}$ is a nonzero ideal in $\mathcal{O}_k$, then there exists a vector $\mathbf{x} \in (\mathcal{O}_k)^N$ such that*

$$A\mathbf{x} \in (\mathcal{I})^M \quad \textit{and} \quad 0 < \prod_{v|\infty} |\mathbf{x}|_v \leq c_k \prod_{v\nmid\infty} H_v(\mathcal{A}_v)^{1/N}.$$

In this case, if $\{\mathfrak{e}_v\}_{v\nmid\infty}$ is the divisor associated with $\mathcal{I}$, then $\mathfrak{e}_v \geq 0$ for all v. This, together with our normalization of H_v and the fact that A is over $\mathcal{O}_k$, implies that

$$\prod_{v\nmid\infty} H_v(\mathcal{A}_v) \leq \operatorname{Norm}(\mathcal{I})^{M/d} \ .$$

Thus Corollary 5 immediately provides a number field analogue of Theorem 2. Moreover, we show in Section 5 that Theorem 3 and Corollary 5 are identical in the case of $k = \mathbf{Q}$, $\mathcal{O}_k = \mathbf{Z}$. We also provide examples over $\mathbf{Q}$ for which there is equality in (iii) of Theorem 4.

Another application of Theorem 4 may be given in the context of the subspace version of Siegel's lemma. Let

$$\mathcal{N} = \left\{\mathbf{x} \in k^N : A\mathbf{x} = \mathbf{0}\right\}$$

be the nullspace of dimension $N - M$ of A. The Bombieri and Vaaler [**3**, Theorem 9] refinement of Siegel's lemma states that there exists a basis for $\mathcal{N}$ for which the product of the heights of the basis vectors is

relatively small. In particular they show that there exist $N-M$ linearly independent vectors $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_{N-M}$ in $(\mathcal{O}_k)^N$ so that $A\mathbf{x}_l = \mathbf{0}$ for all $l = 1, 2, \dots, N-M$ and

$$\prod_{l=1}^{N-M} h(\mathbf{x}_l) \le c_k^{N-M} H(A),$$

where $H(A) = \prod_v H_v(A)$ is the global height on the Grassmann coordinates of A and $h(\mathbf{x})$ is the projective height of $\mathbf{x}$ in k^N (see [7] for a recent refinement of this formulation of Siegel's lemma). We may now use Theorem 4 to show the existence of M linearly independent vectors $\mathbf{y}_1, \mathbf{y}_2, \dots, \mathbf{y}_M$ in $k^N \setminus \mathcal{N}$ so that $A\mathbf{y}_m$ is in some arithmetical sense small for each $m = 1, 2, \dots, M$ and with the 'size' of the $\mathbf{y}_m$'s under control. Thus, the $\mathbf{y}_m$'s are small vectors that are close to the subspace $\mathcal{N}$. In particular we have

Corollary 6. *Let A be an $M \times N$ matrix over k of $\operatorname{rank}(A) = M < N$. If $\mathcal{I}$ and $\mathcal{J}$ are fractional ideals in k and $\mathcal{A}_v = \mathcal{A}_v(A, \mathcal{I}, \mathcal{J})$ the associated $(M+N) \times N$ matrix over k_v for each nonarchimedean place v, then there exist M linearly independent vectors $\mathbf{y}_1, \mathbf{y}_2, \dots, \mathbf{y}_M$ in $(\mathcal{J})^N$ so that $A\mathbf{y}_m \in (\mathcal{I})^M$, $A\mathbf{y}_m \neq \mathbf{0}$ for $m = 1, 2, \dots, M$ and*

$$\prod_{m=1}^{M} \prod_{v|\infty} |\mathbf{y}_m|_v \le c_k^N \operatorname{Norm}(\mathcal{J})^{(M-N)/d} \prod_{v \nmid \infty} H_v(\mathcal{A}_v) \ .$$

As an illustration of Corollary 6, we consider the case when $k = \mathbf{Q}$, $\mathcal{I} = m\mathbf{Z}$, where $m > 1$ is an integer and $\mathcal{J} = \mathbf{Z}$. Then by the corollary, there exists a vector $\mathbf{y} \in \mathbf{Z}^N$ such that

$$A\mathbf{y} \equiv \mathbf{0} \pmod{m}, \qquad A\mathbf{y} \neq \mathbf{0}$$

with

$$0 < |\mathbf{y}| \le \prod_{p \text{ prime}} H_p(\mathcal{A}_p)^{1/M}.$$

As will be shown in Section 5, the previous inequality is equivalent to

$$|\mathbf{y}| \le m \prod_{i=1}^{M} \gcd(m, d_i)^{-1/M}, \tag{1.1}$$

where $d_1, d_2, \ldots, d_M$ are the invariant factors associated with A. Thus, inequality (1.1) is nontrivial whenever $\prod_{i=1}^{M} \gcd(m, d_i) > 2^M$.

2. Heights and measures. Let k be an algebraic number field of degree d over $\mathbf{Q}$ with ring of integers $\mathcal{O}_k$. For each place v of k, we let k_v denote the completion of k with respect to v and for each nonarchimedean place v we write $\mathcal{O}_v = \{x \in k_v : |x|_v \leq 1\}$ for the ring of v-adic integers. We also let $d_v = [k_v : \mathbf{Q}_v]$ denote the local degree. If v is an infinite place we write $\| \ \|_v$ for the usual Euclidean absolute value on k_v. If v is a finite place then $\| \ \|_v$ denotes the unique absolute value on k_v which extends the usual p-adic absolute value on $\mathbf{Q}_p$, where $v \mid p$. We normalize a second absolute value $| \ |_v$ at each place v by setting $| \ |_v = \| \ \|_v^{d_v/d}$. It follows that these absolute values satisfy the *product formula*: $\prod_v |\alpha|_v = 1$ for all $\alpha \in k$, $\alpha \neq 0$. We define the field constant c_k by

$$c_k = \left(\left(\frac{2}{\pi} \right)^s |\Delta_k|^{1/2} \right)^{1/d}, \tag{2.1}$$

where s is the number of complex places of k and Δ_k is the discriminant of k.

Let $\mathcal{I}$ be a fractional ideal in k, that is, $\mathcal{I}$ is a nonzero finitely generated $\mathcal{O}_k$-submodule of k. We recall that there is a natural one-to-one correspondence between fractional ideals $\mathcal{I}$ and divisors $\{\mathfrak{e}_v\}_{v \nmid \infty}$ given by

$$\mathcal{I} = \prod_{v \nmid \infty} \mathcal{P}_v^{\mathfrak{e}_v} \ ,$$

where the $\mathcal{P}_v$'s are prime ideals in $\mathcal{O}_k$. We define the *norm of* $\mathcal{I}$, $\mathrm{Norm}(\mathcal{I})$, by

$$\mathrm{Norm}(\mathcal{I}) = \prod_{v \nmid \infty} \|\pi_v\|_v^{-d_v \mathfrak{e}_v},$$

where π_v is a generator for the unique maximal ideal in $\mathcal{O}_v$. For our purposes, it will be convenient to view $\mathcal{I}$ 'geometrically' as follows. Given $\mathcal{I}$ and its associated divisor $\{\mathfrak{e}_v\}_{v \nmid \infty}$, we have

$$\mathcal{I} = \{x \in k : \|x\|_v \leq \|\pi_v\|_v^{\mathfrak{e}_v} \text{ for all } v \nmid \infty\} \ . \tag{2.2}$$

Let

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_N \end{pmatrix}$$

be a column vector in $(k_v)^N$. We extend the absolute values $\| \ \|_v$ and $| \ |_v$ to $(k_v)^N$ by defining

$$\|\mathbf{x}\|_v = \max_{1 \le n \le N} \{\|x_n\|_v\}$$

and $|\mathbf{x}|_v = \|\mathbf{x}\|_v^{d_v/d}$ for all v.

Let $X = (x_{mn})$ be an $M \times N$ matrix over k_v. If $J \subseteq \{1, 2, \dots, M\}$ is a subset of cardinality $|J| = L$, we write

$$_JX = (x_{mn}), \qquad m \in J, \quad n = 1, 2, \dots, N,$$

for the corresponding $L \times N$ submatrix. Similarly, if $I \subseteq \{1, 2, \dots, N\}$ is a subset of cardinality $|I| = L$, we write

$$X_I = (x_{mn}), \qquad m = 1, 2, \dots, M, \quad n \in I \ ,$$

for the corresponding $M \times L$ submatrix. Now suppose the $\operatorname{rank}(X) = M \le N$. We define the *local height* $H_v(X)$ on the Grassmann coordinates of X as follows:

(i) If $v \mid \infty$ then

$$H_v(X) = \left(\sum_{|I|=M} \| \det X_I \|_v^2 \right)^{d_v/2d}.$$

(ii) If $v \nmid \infty$ then

$$H_v(X) = \max_{|I|=M} \{| \det X_I |_v\}.$$

The local nonarchimedean heights are of fundamental importance in the current work.

We select a Haar measure β_v on the additive group of k_v by the following normalization:

(i) If $k_v \cong \mathbf{R}$ then β_v is the usual Lebesgue measure on $\mathbf{R}$.

(ii) If $k_v \cong \mathbf{C}$ then β_v is Lebesgue measure on the complex plane multiplied by 2.

(iii) If $v \nmid \infty$ we require that $\beta_v(\mathcal{O}_v) = |\mathcal{D}_v|_v^{d/2}$, where $\mathcal{D}_v$ is the local different of k at v.

We write $k_{\mathbf{A}}$ for the adèle ring of k and β for the normalized Haar measure on $k_{\mathbf{A}}$ which is induced by the product measure $\prod_v \beta_v$. If $(k_{\mathbf{A}})^N$ is the N-fold product of adèle spaces we write V for the product Haar measure β^N on $(k_{\mathbf{A}})^N$. We remark that in the geometry of numbers over the adèles, the Haar measure V plays the role of volume in the classical theory.

We may embed $k^N \hookrightarrow (k_{\mathbf{A}})^N$ via the usual diagonal embedding. It follows that k^L is discrete and the quotient $(k_{\mathbf{A}})^N/k^N$ is compact with induced Haar measure

$$\bar{V}\left((k_{\mathbf{A}})^N/k^N\right) = 1$$

(see, for example [**15**]). The vector space k^N plays the role of the lattice. An overview of recent results in the geometry of numbers over the adèles may be found in [**5**] or [**6**].

For each place v of k let $R_v \subseteq (k_v)^N$ be a nonempty set. If $v \mid \infty$ we assume that R_v is open, convex and symmetric. If $v \nmid \infty$ we assume that R_v is a k_v-lattice, that is, a compact open $\mathcal{O}_v$-module. We further assume that for almost all finite v, $R_v = (\mathcal{O}_v)^N$. We define the set

$$\mathcal{R} = \prod_v R_v.$$

From our previous assumptions it is clear that $\mathcal{R} \subseteq (k_{\mathbf{A}})^N$. We call a subset $\mathcal{R}$ *admissible* if it has the form described above. For $\sigma > 0$ we define the dilation $\sigma\mathcal{R}$ by

$$\sigma\mathcal{R} = \prod_{v\mid\infty} (\sigma R_v) \times \prod_{v\nmid\infty} R_v \ .$$

We now recall the definition of the successive minima $0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_N < \infty$ of $\mathcal{R}$. We define

$$\lambda_n = \inf\left\{\sigma > 0 : \sigma\mathcal{R} \cap k^N \text{ contains } n \text{ linearly independent vectors}\right\}.$$

The adelic analogue of Minkowski's successive minima theorem (see [**3**, Theorem 3]) states that

$$(\lambda_1\lambda_2\cdots\lambda_N)^d V(\mathcal{R}) \le 2^{dN}. \tag{2.3}$$

3. Proof of Theorem 4. For each place v of k we define the set $R_v \subseteq (k_v)^N$ as follows. If $v \mid \infty$ then

$$R_v = \{\mathbf{x} \in (k_v)^N : \|\mathbf{x}\|_v < 1\}\ .$$

If $v \nmid \infty$ then

$$R_v = \{\mathbf{x} \in (k_v)^N : \|\mathcal{A}_v\mathbf{x}\|_v \le 1\},$$

where $\mathcal{A}_v$ is the $(M+N)\times N$ augmented matrix

$$\mathcal{A}_v = \begin{pmatrix} \pi_v^{-\mathfrak{e}_v} A \\ - \ - \ - \\ \pi_v^{-\mathfrak{f}_v}\mathbf{1}_N \end{pmatrix}.$$

We note that for almost all v, $R_v = (\mathcal{O}_v)^N$. We define $\mathcal{R} \subseteq (k_{\mathbf{A}})^N$ be the admissible set $\mathcal{R} = \prod_v R_v$.

For $v \mid \infty$, we easily have

$$\beta_v^N(R_v) = \begin{cases} 2^N & \text{if } v \text{ is real,} \\ (2\pi)^N & \text{if } v \text{ is complex.} \end{cases}$$

For $v \nmid \infty$, R_v is a nonarchimedean cube slice and thus from equations (4.8) and (4.9) of [**3**] we have

$$\beta_v^N(R_v) = H_v(\mathcal{A}_v)^{-d}\beta_v^N\left((\mathcal{O}_v)^N\right).$$

Since

$$\prod_{v\nmid\infty} |\mathcal{D}_v|_v^{-d} = |\Delta_k|,$$

we conclude that

$$V(\mathcal{R}) = 2^{dN}(\pi/2)^{sN}|\Delta_k|^{-N/2}\prod_{v\nmid\infty} H_v(\mathcal{A}_v)^{-d}.$$

Hence by (2.1) and inequality (2.3),

$$\lambda_1\lambda_2\cdots\lambda_N \le c_k^N \prod_{v\nmid\infty} H_v(\mathcal{A}_v). \tag{3.1}$$

Let $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_N$ be linearly independent vectors in k^N associated with the successive minima of $\mathcal{R}$. That is, for $\lambda > \lambda_n$,

$$\{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n\} \subseteq \lambda\mathcal{R},$$

for $n = 1, 2, \ldots, N$. Given that dilation of admissible sets only occurs at the archimedean places, we have that for all $n = 1, 2, \ldots, N$,

$$\|\mathcal{A}_v\mathbf{x}_n\|_v \le 1 \quad \text{for all places } v \nmid \infty. \tag{3.2}$$

If we consider the lower $N \times N$ portion of the augmented matrix $\mathcal{A}_v$, we conclude that $\|\mathbf{x}_n\|_v \le \|\pi_v\|_v^{\mathfrak{f}_v}$ for all $v \nmid \infty$. By (2.2), we have that $\mathbf{x}_n \in (\mathcal{J})^N$ for all $n = 1, 2, \ldots, N$ which establishes part (i) of the theorem. In view of the top $N \times N$ portion of the augmented matrix $\mathcal{A}_v$, (3.2) implies that

$$\|A\mathbf{x}_n\|_v \le \|\pi_v\|_v^{\mathfrak{e}_v},$$

for all $v \nmid \infty$. Thus, $A\mathbf{x}_n \in (\mathcal{I})^M$ for all $n = 1, 2, \ldots, N$, and hence part (ii) holds.

Finally, for $v \mid \infty$, we have $\|\mathbf{x}_n\|_v \le \lambda_n$ for $n = 1, 2, \ldots, N$. Thus for each n,

$$\begin{aligned}\prod_{v\mid\infty} |\mathbf{x}_n|_v &= \prod_{v\mid\infty} \|\mathbf{x}_n\|_v^{d_v/d} \\ &\le \prod_{v\mid\infty} \lambda_n^{d_v/d} \\ &= \lambda_n^{\sum_{v\mid\infty} d_v/d} \\ &= \lambda_n.\end{aligned}$$

The inequality of (iii) now follows from (3.1), which completes the proof. □

4. Proof of Corollary 6. If we let $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_N$ be as in Theorem 4, then it follows from the previous proof that, for each n,

$$\prod_v |\mathbf{x}_n|_v = \prod_{v|\infty} |\mathbf{x}_n|_v \prod_{v\nmid\infty} |\mathbf{x}_n|_v \le \lambda_n \operatorname{Norm}(\mathcal{J})^{-1/d}.$$

However, by the product formula, as $\mathbf{x}_n$ is not the zero vector, we have $1 \le \prod_v |\mathbf{x}_n|_v$. This yields

$$\operatorname{Norm}(\mathcal{J})^{1/d} \le \lambda_n. \tag{4.1}$$

Inequalities (3.1) and (4.1) imply that

$$\lambda_{N-M+1}\lambda_{N-M+2}\cdots\lambda_N \le c_k^N \operatorname{Norm}(\mathcal{J})^{(M-N)/d} \prod_{v\nmid\infty} H_v(\mathcal{A}_v).$$

Plainly at most $N - M$ of the vectors $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_N$ are contained in the null space of A. As the successive minima are nondecreasing, the corollary now follows by selecting any M vectors from $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_N$ which are not in the null space of A. □

5. Remarks in the rational number field case. We begin by demonstrating that in the case $k = \mathbf{Q}$, Corollary 5 is identical to Theorem 3. Suppose that A is an $M \times N$ matrix over $\mathbf{Z}$ of full rank M and $\mathcal{I} = m\mathbf{Z}$, where $m > 0$ is an integer with prime factorization $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_L^{\alpha_L}$, $\alpha_l > 0$ for all l. Corollary 5 asserts the existence of a vector $\mathbf{x} \in \mathbf{Z}^N$ such that $A\mathbf{x} \equiv \mathbf{0} \pmod m$ and

$$0 < |\mathbf{x}| \le \prod_{p \text{ prime}} H_p(\mathcal{A}_p)^{1/N}. \tag{5.1}$$

Plainly $H_p(\mathcal{A}_p) = 1$ for all $p \nmid m$ and therefore we need only investigate $H_p(\mathcal{A}_p)$ for $p \mid m$, that is, $p \in \{p_1, \ldots, p_L\}$.

Let $d_1, d_2, \ldots, d_M$ be the invariant factors associated with A. It follows that for each r, $1 \le r \le M$, (see, for example, [**10**, Chapter VI, Section 3])

$$d_r = \prod_{p \text{ prime}} \left\{ \frac{\max_{|J|=r-1} \{H_p({}_J A)\}}{\max_{|I|=r} \{H_p({}_I A)\}} \right\}.$$

Therefore,

$$|d_r|_p = \left(\frac{\max_{|J|=r-1} \{H_p({}_J A)\}}{\max_{|I|=r} \{H_p({}_I A)\}} \right)^{-1},$$

or alternatively,

$$\max_{|I|=r} \{H_p({}_I A)\} = |d_r|_p \left(\max_{|J|=r-1} \{H_p({}_J A)\} \right). \tag{5.2}$$

Suppose now that $p^\alpha \in \{p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_L^{\alpha_L}\}$ is an arbitrary fixed element. Then

$$\mathcal{A}_p = \begin{pmatrix} p^{-\alpha} A \\ - - - \\ \mathbf{1}_N \end{pmatrix}.$$

Thus by successive applications of the reduction (5.2) we have

$$\begin{aligned} H_p(\mathcal{A}_p) &= \max_{0 \le r \le M} \left\{ p^{\alpha r} \left\{ \max_{|I|=r} \{H_p({}_I A)\} \right\} \right\} \\ &= \max_{0 \le r \le M} \left\{ p^{\alpha r} |d_r|_p \left\{ \max_{|J|=r-1} \{H_p({}_J A)\} \right\} \right\} \\ &= \max_{0 \le r \le M} \left\{ p^{\alpha r} |d_r d_{r-1}|_p \left\{ \max_{|J|=r-2} \{H_p({}_J A)\} \right\} \right\} \\ &\vdots \\ &= \max_{0 \le r \le M} \{ p^{\alpha r} |d_r d_{r-1} \cdots d_1|_p \}. \end{aligned}$$

For each $r = 1, 2, \dots, M$, we let β_r denote the nonnegative integer so that $|d_r|_p = p^{-\beta_r}$. It follows from well-known properties of the invariant factors that $0 \le \beta_1 \le \beta_2 \le \cdots \le \beta_M$. Therefore the above computation for $H_p(\mathcal{A}_p)$ may be expressed as

$$H_p(\mathcal{A}_p) = \max_{0 \le r \le M} \left\{ p^{\alpha r - \sum_{i=1}^r \beta_i} \right\}. \tag{5.3}$$

Next let T be the largest index so that $\beta_T \le \alpha$. Hence (5.3) reveals

$$\begin{aligned} H_p(\mathcal{A}_p) &= p^{\alpha T - \sum_{i=1}^T \beta_i} \\ &= p^{\alpha M - \sum_{i=1}^M \max\{\alpha, \beta_i\}} \\ &= p^{\alpha M} \left\{ \prod_{i=1}^M \gcd(p^\alpha, d_i) \right\}^{-1}. \end{aligned}$$

Given the factorization of m and the fact that $H_p(\mathcal{A}_p) = 1$ for all primes $p \nmid m$, the previous identity implies that

$$\prod_{p \text{ prime}} H_p(\mathcal{A}_p)^{1/N} = m^{M/N} \left\{ \prod_{i=1}^{M} \gcd(m, d_i) \right\}^{-1/N}.$$

Therefore the upper bound occurring in (5.1) is identical to the upper bound of Theorem 3.

We now produce examples to illustrate that the upper bound of Theorem 4 is sharp. Let $q_1 < q_2$ be two primes, $\mathcal{I} = (q_1^2 q_2)\mathbf{Z}$, $\mathcal{J} = \mathbf{Z}$ and A be given by

$$A = \begin{pmatrix} q_1 q_2 & 0 & 1 \\ 0 & q_1 q_2 & 1 \end{pmatrix}.$$

Thus by Theorem 4 there exist linearly independent vectors $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ in $\mathbf{Z}^3$ such that

$$A\mathbf{x}_n \equiv \mathbf{0} \pmod{q_1^2 q_2}, \tag{5.4}$$

and

$$\prod_{n=1}^{3} |\mathbf{x}_n| \leq \prod_{p \text{ prime}} H_p(\mathcal{A}_p). \tag{5.5}$$

It is easily seen that $H_{q_1}(\mathcal{A}_{q_1}) = q_1^3$, $H_{q_2}(\mathcal{A}_{q_2}) = q_2$ and $H_p(\mathcal{A}_p) = 1$ for all other primes p. Therefore the upper bound in (5.5) is simply $q_1^3 q_2$. One may verify that the smallest three linearly independent vectors in $\mathbf{Z}^3$ that satisfy (5.4) are

$$\mathbf{x}_1 = \begin{pmatrix} q_1 \\ 0 \\ 0 \end{pmatrix}, \qquad \mathbf{x}_2 = \begin{pmatrix} 0 \\ q_1 \\ 0 \end{pmatrix}, \qquad \mathbf{x}_3 = \begin{pmatrix} -1 \\ -1 \\ q_1 q_2 \end{pmatrix},$$

and hence $|\mathbf{x}_1|\,|\mathbf{x}_2|\,|\mathbf{x}_3| = q_1^3 q_2$. Thus there is equality in (5.5).

Acknowledgments. The author wishes to thank Professors W.M. Schmidt and R.I. Mizner for their helpful comments regarding this work.

REFERENCES

1. L. Aubry, *Un théorème d'arithmétique*, Mathesis **3** (1913).

2. R. Ballieu, *sur des congruences arithmétiques*, Bulletin de la Classe des Sciences de l'Académie Royale de Belgique **34** (1948), 39–45.

3. E. Bombieri and J. Vaaler, *On Siegel's lemma*, Invent. Math. **73** (1983), 11–32.

4. A. Brauer and R.L. Reynolds, *On a theorem of Aubry-Thue*, Canad. J. Math. **3** (1951), 367–374.

5. E.B. Burger, *Homogeneous diophantine approximation in S-integers*, Pacific J. Math. **152** (1992), 211–253.

6. ———, *Badly approximable systems and inhomogeneous approximation over number fields*, in *Number theory with an emphasis on the Markoff spectrum* (A. Pollington and W. Moran, eds.), Marcel Dekker, New York, 1993.

7. E.B. Burger and J.D. Vaaler, *On the decomposition of vectors over number fields*, J. Reine Angew. Math. **435** (1993), 197–219.

8. T. Cochrane, *Small solutions of congruences over algebraic number fields*, Illinois J. Math. **31** (1987), 618–625.

9. S.M. De Backer, *Solutions modérées d'un système de congruences du premier degré pour un module premier p*, Bulletin de la Classe des Sciences de l'Académie Royale de Belgique **34** (1948), 46–51.

10. F.R. Gantmacher, *The theory of matrices*, Volume One, Chelsea Publishing Company, New York, 1960.

11. R.B. McFeat, *Geometry of numbers in adèle spaces*, Dissertationes Math. (Rozprawy Mat.) **88** (1971), 1–49.

12. T. Nagell, *Sur un théorème d'Axel Thue*, Ark. Math. **1** (1951), 489–491.

13. A. Thue, *Et bevis for at lignigen $A^3 + B^3 = C^3$ er remulig i hele fra nul forsk jellige tal A, B og C*, Archiv. for Math. og Naturvid **34** (1917),

14. J.M. Vinogradov, *On a general theorem concerning the distribution of the residues and non-residues of powers*, Trans. Amer. Math. Soc. **29** (1927), 209–217.

15. A. Weil, *Basic number theory*, Springer, New York, 1974.

Department of Mathematics, Williams College, Williamstown, Massachusetts 01267
E-mail address: Edward.B.Burger@williams.edu