# ON SYSTEMS OF DIAGONAL FORMS

## MICHAEL P. KNAPP

### Abstract

In this paper we consider systems of diagonal forms with integer coefficients in which each form has a different degree. Every such system has a nontrivial zero in every $p$-adic field $\mathbb{Q}_p$ provided that the number of variables is sufficiently large in terms of the degrees. While the number of variables required grows at least exponentially as the degrees and number of forms increase, it is known that if $p$ is sufficiently large then only a small polynomial bound is required to ensure zeros in $\mathbb{Q}_p$. In this paper we explore the question of how small we can make the prime $p$ and still have a polynomial bound. In particular, we show that we may allow $p$ to be smaller than the largest of the degrees.

## 1. Introduction

In this paper, we study conditions under which the system of homogeneous equations

$$
\begin{array}{ccccccccc}
F_1(\mathbf{x}) & = & a_{11}x_1^{k_1} & + & \cdots & + & a_{1s}x_s^{k_1} & = & 0 \\
\vdots & & \vdots & & & & \vdots & & \\
F_R(\mathbf{x}) & = & a_{R1}x_1^{k_R} & + & \cdots & + & a_{Rs}x_s^{k_R} & = & 0
\end{array}
\tag{1}
$$

with $a_{ij} \in \mathbb{Z}$ and $k_1, \ldots, k_R \in \mathbb{Z}^+$ is guaranteed to have a nontrivial solution in $p$-adic integers. By nontrivial, we mean simply that at least one of the variables is not equal to zero. A conjecture commonly attributed to Artin suggests that regardless of the values of the coefficients, a nontrivial zero in $\mathbb{Z}_p^s$ should exist for each prime $p$ provided only that

we have

$$s > \sum_{i=1}^{R} k_i^2.$$

If $R = 1$, then Davenport & Lewis [5] have shown that this bound is correct. Unfortunately, the following theorem of Lewis & Montgomery [8] shows that this conjecture is false, and that any such bound on $s$ must in fact exhibit exponential growth.

THEOREM 1 (**Lewis-Montgomery**). *Suppose $p$ is an odd prime. Let $M$ be a positive integer, and let $\mathfrak{M}$ be a set of $K$ integers in the range $[M, 2M - 1]$. Suppose that there are $s$ integers $x_1, \ldots, x_s$, not all divisible by $p$, such that*

$$x_1^{(p-1)m} + \cdots + x_s^{(p-1)m} \equiv 0 \pmod{p^{(p-1)M}}$$

*for all $m$ in $\mathfrak{M}$. Then $s \geq p^K$.*

On the other hand, Ax & Kochen [1] have shown that if we ask only that a nontrivial solution exists in $\mathbb{Z}_p^s$ for $p$ sufficiently large, then the Artin bound is sufficient. It is therefore an interesting problem to determine how small we can take the prime $p$ to be before exponential growth is required. In particular, how small can we make $p$ and still obtain polynomial bounds for $s$?

In this paper, we explore this problem in the situation where the degrees of the polynomials are all different. In order to write down our conclusions, we introduce the following notational convention. Let $\Gamma_p^*(k_1, \ldots, k_R)$ be the smallest number such that any system of forms as in (1) has a nontrivial solution in $\mathbb{Z}_p^s$ whenever $s \geq \Gamma_p^*(k_1, \ldots, k_R)$. For example, if $k_1, \ldots, k_R$ are fixed, then the result of Ax & Kochen above states that one has

$$\Gamma_p^*(k_1, \ldots, k_R) \leq 1 + \sum_{i=1}^{R} k_i^2$$

2

for sufficiently large $p$. The purpose of this paper is to prove the following theorem.

THEOREM 2. *Suppose that $R \geq 2$ and let $k_1 > k_2 > \cdots > k_R$ be positive integers. For a fixed prime $p$, define numbers $\tau_i$ and $\tilde{k}_i$, $(1 \leq i \leq R)$, so that $k_i = p^{\tau_i} \tilde{k}_i$ with $(p, \tilde{k}_i) = 1$.*

*i) Define*

$$S_1 = \sum_{i=1}^{R} \tilde{k}_i \frac{p^{\tau_i+1} - 1}{p - 1}.$$

*If $p > k_1 - k_R + 1$, then we have*

$$\Gamma_p^*(k_1, \ldots, k_R) \leq (S_1 + 1) \sum_{i=1}^{R} ik_i - \sum_{i=1}^{R} k_i + R.$$

*This implies the bound*

$$\Gamma_p^*(k_1, \ldots, k_R) \leq \frac{3}{2} R \left( \sum_{i=1}^{R} k_i \right)^2 + (R - 1) \left( \sum_{i=1}^{R} k_i \right) + R$$

*for such $p$.*

*ii) Define*

$$S_2 = \sum_{i=1}^{R} \tilde{k}_i \frac{p^{\tau_i+3} - 1}{p - 1}.$$

*If we have*

$$p > 1 + \max \left\{ 1, k_1 - k_{R-1}, \frac{k_1 - k_R}{2} \right\},$$

*then we have*

$$\Gamma_p^*(k_1, \ldots, k_R) \leq (S_2 + 1) \sum_{i=1}^{R} ik_i - \sum_{i=1}^{R} k_i + R.$$

*This implies that for these $p$ we have the bound*

$$\Gamma_p^*(k_1, \ldots, k_R) \leq \frac{3}{2} R(k_1 - k_R + 1)^2 \left( \sum_{i=1}^{R} k_i \right)^2 + (R - 1) \left( \sum_{i=1}^{R} k_i \right) + R.$$

*This shows in particular that polynomial bounds are possible for primes smaller than the largest degree.*

We prove this theorem through a method similar to the one used in [7]. First we apply a normalization process which shows that we need only consider systems which have certain desirable properties. Then we will consider the system (1), with each equation reduced modulo a power of $p$, and determine a number of variables which guarantees that this system of congruences will have a nonsingular solution. Finally, we will lift this solution of congruences to a nontrivial solution of (1) in $\mathbb{Z}_p^s$ through a version of Hensel's Lemma.

## 2. Normalization

In this section we describe the process by which we normalize the system of equations and derive a few properties of normalized systems. Our normalization process essentially combines the two used by Wooley in [10] and [11]. Suppose that $\mathbf{F} = (F_1, \ldots, F_R)$ is a system of additive forms as in (1), and that the prime $p$ is fixed. We define two fundamental operations on $\mathbf{F}$. First, we may write

$$\mathbf{F}' = \mathbf{b}\mathbf{F} = (b_1 F_1, \ldots, b_R F_R)$$

for some vector $\mathbf{b}$ of nonzero rational numbers. Second, we may make a change of variables of the form $x_i \mapsto p^{-v_i} x_i$, where the $v_i$ are rational integers, yielding a system of the form

$$\mathbf{F}'' = \mathbf{F}(p^{v_1} x_1, \ldots, p^{v_s} x_s).$$

Note that these operations commute. A system $\mathbf{G}$ with integer coefficients is said to be *equivalent* to $\mathbf{F}$ if $\mathbf{G}$ can be obtained from $\mathbf{F}$ through a combination of the above operations, i.e. if we can write

$$\mathbf{G} = \mathbf{b}\mathbf{F}(p^{v_1} x_1, \ldots, p^{v_s} x_s).$$

Now we wish to define a function $\partial(\mathbf{F})$ whose value depends on the coefficients of $F_1, \ldots, F_R$ and which behaves nicely under the fundamental operations. Unfortunately, this will require a fair amount of notation. Define $K = k_1 k_2 \cdots k_R$ and for each $i$ let

4

$k_i' = K/k_i$. For any fixed integer $r$ with $R \le r \le s$, we define

$$S_r = \{(j_1, \ldots, j_R) \in \{1, \ldots, r\}^R : j_i \ne j_{i'} \text{ when } i \ne i'\}$$

and note that if we set $L = |S_r|$, then we have

$$L = r(r-1)\cdots(r-R+1).$$

For each $\sigma = (j_1, \ldots, j_R) \in S_r$, write

$$D_\sigma(\mathbf{F}) = \det\left(\left[a_{ij_m}^{k_i'}\right]_{1 \le i, m \le R}\right).$$

Further, for fixed numbers $m_1, \ldots, m_{R-1}$ with $r+1 \le m_1 \le \cdots \le m_{R-1} \le s$, we define

$$M_1 = \{r+1, \ldots, m_1\}$$
$$M_2 = \{m_1+1, \ldots, m_2\}$$
$$\vdots$$
$$M_R = \{m_{R-1}+1, \ldots, s\},$$

taking $M_i$ to be empty if $m_i = m_{i-1}$. Also, for $i = 1, \ldots, R$, we set

$$N_i = \frac{RL}{r}k_i'.$$

Finally, we define

$$\partial(\mathbf{F}) = \prod_{\sigma \in S_r} D_\sigma(\mathbf{F}) \prod_{j \in M_1} a_{1j}^{N_1} \prod_{j \in M_2} a_{2j}^{N_2} \cdots \prod_{j \in M_R} a_{Rj}^{N_R}.$$

We now show that $\partial(\mathbf{F})$ behaves nicely under the fundamental operations.

LEMMA 3. *Suppose that* $\mathbf{F}$ *is a system of forms as in (1) with integral coefficients. Then the following statements are true.*

*i) If we set* $\mathbf{F}' = \mathbf{b}\mathbf{F} = (b_1 F_1, \ldots, b_R F_R)$, *then we have*

$$\partial(\mathbf{F}') = \left(\prod_{i=1}^{R} b_i^{(L+|M_i|RL/r)k_i'}\right)\partial(\mathbf{F}).$$

*ii) If we set* $\mathbf{F}'' = \mathbf{F}\left(p^{v_1}x_1, \ldots, p^{v_s}x_s\right)$, *then we have*

$$\partial(\mathbf{F}'') = p^{RLKv/r}\partial(\mathbf{F}),$$

*where we have set* $v = v_1 + \cdots + v_s$.

**Proof.** To prove the first statement, let $\mathbf{F}'$ be the system

$$F_i' = a_{i1}' x_1^{k_i} + \cdots + a_{is}' x_s^{k_i} \qquad (i = 1, \ldots, R).$$

If $\mathbf{F}' = \mathbf{bF}$, then we have $a_{ij}' = b_i a_{ij}$ for each pair $i, j$. If $\sigma = (j_1, \ldots, j_R) \in S_r$, then

$$D_\sigma(\mathbf{F}') = \det\left( \left[ b_i^{k_i'} a_{ij_m}^{k_i'} \right]_{i,m} \right)$$
$$= b_1^{k_1'} \cdots b_R^{k_R'} \det\left( \left[ a_{ij_m}^{k_i'} \right]_{i,m} \right)$$
$$= b_1^{k_1'} \cdots b_R^{k_R'} D_\sigma(\mathbf{F}),$$

whence we obtain

$$\prod_{\sigma \in S_r} D_\sigma(\mathbf{F}') = \prod_{\sigma \in S_r} b_1^{k_1'} \cdots b_R^{k_R'} D_\sigma(\mathbf{F}) = b_1^{k_1' L} \cdots b_R^{k_R' L} \prod_{\sigma \in S_r} D_\sigma(\mathbf{F}). \qquad (2)$$

Moreover, for each $i = 1, \ldots, R$, we have

$$\prod_{j \in M_i} \left( a_{ij}' \right)^{N_i} = \prod_{j \in M_i} b_i^{N_i} a_{ij}^{N_i} = b_i^{|M_i| N_i} \prod_{j \in M_i} a_{ij}^{N_i} = b_i^{|M_i| RL k_i'/r} \prod_{j \in M_i} a_{ij}^{N_i}. \qquad (3)$$

Putting (2) and (3) together, we obtain

$$\partial(\mathbf{F}') = \left( b_1^{k_1' L} \cdots b_R^{k_R' L} \prod_{i=1}^{R} b_i^{|M_i| RL k_i'/r} \right) \partial(\mathbf{F})$$
$$= \left( \prod_{i=1}^{R} b_i^{(L + |M_i| RL/r) k_i'} \right) \partial(\mathbf{F}),$$

as desired.

In order to prove the second statement, we let $\mathbf{F}''$ be the system

$$F_i'' = a_{i1}'' x_1^{k_i} + \cdots + a_{is}'' x_s^{k_i} \qquad (i = 1, \ldots, R).$$

If $\mathbf{F}'' = \mathbf{F}(p^{v_1} x_1, \ldots, p^{v_s} x_s)$, then we have $a_{ij}'' = p^{k_i v_j} a_{ij}$ for each pair $i, j$. If $\sigma = (j_1, \ldots, j_R) \in S_r$, then we have

$$D_\sigma(\mathbf{F}'') = \det\left( \left[ \left( a_{ij_m}'' \right)^{k_i'} \right]_{i,m} \right)$$
$$= \det\left( \left[ p^{K v_{j_m}} a_{ij_m}^{k_i'} \right]_{i,m} \right)$$
$$= p^{K v_{j_1}} \cdots p^{K v_{j_R}} \det\left( \left[ a_{ij_m}^{k_i'} \right]_{i,m} \right)$$
$$= p^{K v_{j_1}} \cdots p^{K v_{j_R}} D_\sigma(\mathbf{F}).$$

6

Therefore we have

$$\prod_{\sigma \in S_r} D_\sigma(\mathbf{F}'') = \prod_{\sigma=(j_1,\ldots,j_R) \in S_r} p^{Kv_{j_1}} \cdots p^{Kv_{j_R}} D_\sigma(\mathbf{F})$$

$$= \prod_{\sigma \in S_r} p^{K(v_{j_1}+\cdots+v_{j_R})} \prod_{\sigma \in S_r} D_\sigma(\mathbf{F})$$

$$= p^{K \sum (v_{j_1}+\cdots+v_{j_R})} \prod_{\sigma \in S_r} D_\sigma(\mathbf{F}),$$

where the sum in the last line is over all $\sigma \in S_r$. Now there are $L$ choices for $\sigma$, and each of $j_1, \ldots, j_r$ appears in $RL/r$ of these choices. Hence we have

$$\sum_{\sigma \in S_r} (v_{j_1} + \cdots + v_{j_R}) = \frac{RL}{r} v_1 + \cdots + \frac{RL}{r} v_r = \frac{RL}{r} \sum{}^* v_j,$$

where we use the notation $\sum^*$ to represent a sum over all $j \le r$. Therefore we have

$$\prod_{\sigma \in S_r} D_\sigma(\mathbf{F}'') = p^{(RLK \sum^* v_j)/r} \prod_{\sigma \in S_r} D_\sigma(\mathbf{F}). \tag{4}$$

Additionally, for each $i$ with $1 \le i \le R$ we have

$$\prod_{j \in M_i} (a_{ij}'')^{N_i} = \prod_{j \in M_i} \left( p^{k_i v_j} a_{ij} \right)^{N_i} = \prod_{j \in M_i} p^{k_i v_j N_i} \prod_{j \in M_i} a_{ij}^{N_i}$$

$$= p^{k_i N_i \sum^i v_j} \prod_{j \in M_i} a_{ij}^{N_i} = p^{(RLK \sum^i v_j)/r} \prod_{j \in M_i} a_{ij}^{N_i}, \tag{5}$$

where $\sum^i$ represents a sum over all $j \in M_i$. Putting (4) and (5) together, we obtain

$$\partial(\mathbf{F}'') = p^{RLK \sum^* v_j/r} p^{RLK \sum^1 v_j/r} \cdots p^{RLK \sum^R v_j/r} \partial(\mathbf{F})$$

$$= p^{RLKv/r} \partial(\mathbf{F}).$$

This completes the proof of the lemma. $\square$

Suppose that $\mathbf{F}$ is a system of additive forms with integer coefficients. A standard argument (see for example page 572 of [6]) shows that in order to prove Theorem 2 for all systems of additive forms, it suffices to prove it for systems such that $\partial(\mathbf{F}) \ne 0$. We say that $\mathbf{F}$ is *p-normalized* if $\partial(\mathbf{F}) \ne 0$ and the power of $p$ dividing $\partial(\mathbf{F})$ is less than or equal to the power of $p$ dividing $\partial(\mathbf{G})$ for any system $\mathbf{G}$ of forms with integer

coefficients which is equivalent to $\mathbf{F}$. Note that since any system is equivalent to one which is $p$-normalized, it suffices to prove the theorem for $p$-normalized systems. We now prove a lemma showing that $p$-normalized systems are explicit in a relatively large number of variables when considered modulo $p$.

LEMMA 4. *Suppose that* $\mathbf{F}$ *is a $p$-normalized system of additive forms. Then the following statements are true.*

*i) If $N$ is the number of variables in $\mathbf{F}$ which are explicit when $\mathbf{F}$ is considered modulo $p$, then one has*

$$N \geq \sum_{i=1}^{R} \left( |M_i| + \frac{r}{R} \right) \frac{1}{k_i}.$$

*ii) If $q_i$ is the number of variables explicit modulo $p$ in the form $F_i$ of degree $k_i$, then one has*

$$q_i \geq \left( |M_i| + \frac{r}{R} \right) \frac{1}{k_i}.$$

**Proof.** To prove the first statement, suppose (by relabeling if necessary) that the variables $x_1, \ldots, x_N$ are the variables which are explicit modulo $p$. Consider the system

$$\mathbf{F}' = p^{-1}\mathbf{F}(px_1, \ldots, px_N, x_{N+1}, \ldots, x_s),$$

which has integer coefficients. The system $\mathbf{F}'$ is obtained from $\mathbf{F}$ via a combination of the fundamental operations with $b_1 = \cdots = b_R = p^{-1}$ and $v = v_1 + \cdots + v_s = N$. Then we have

$$\partial(\mathbf{F}') = \left( p^{RLKN/r} \prod_{i=1}^{R} (p^{-1})^{(L+|M_i|RL/r)k_i'} \right) \partial(\mathbf{F})$$
$$= p^A \partial(\mathbf{F}),$$

where we have set

$$A = \frac{RLKN}{r} - \sum_{i=1}^{R} \left( |M_i| \frac{RL}{r} + L \right) k_i'.$$

Since the system $\mathbf{F}$ is $p$-normalized, we must have $A \geq 0$, and the first part of the lemma follows.

For the second statement, fix $i$ and suppose that the variables in the form $F_i$ which are explicit modulo $p$ are $x_1, \ldots, x_{q_i}$. Consider the system

$$\mathbf{F}'' = \mathbf{b}\mathbf{F}(px_1, \ldots, px_{q_i}, x_{q_i+1}, \ldots, x_s),$$

where $b_i = p^{-1}$ and $b_j = 1$ if $j \neq i$. Note that $\mathbf{F}''$ is a system of forms with integer coefficients. Then we have $v = q_i$ and hence $\partial(\mathbf{F}'') = p^B \partial(\mathbf{F})$, where

$$B = \frac{RLKq_i}{r} - \frac{|M_i|RLk_i'}{r} - Lk_i'.$$

Since the system $\mathbf{F}$ is $p$-normalized and $\mathbf{F}''$ is equivalent to $\mathbf{F}$, we must have $B \geq 0$, and part ii) of the lemma follows. This completes the proof of the lemma. $\square$

## 3. Preliminary Lemmata

In this section we establish some lemmata which will be needed in the proof of Theorem 2. Our first lemma, due to Schanuel [9], provides a bound on the number of variables necessary to solve a system of congruences modulo various powers of a prime $p$.

LEMMA 5. *For $1 \leq i \leq R$, let $F_i$ be a (not necessarily homogeneous) polynomial of degree $k_i$ in $N$ variables with coefficients in $\mathbb{Z}_p$ and no constant term. Also let $T_p = \{x \in \mathbb{Z}_p : x^p = x\}$ be the set of Teichmüller representatives of $\{0, 1, 2, \ldots, p-1\}$. Then the system of equations*

$$F_i(x_1, \ldots, x_N) \equiv 0 \pmod{p^{v_i}} \quad (1 \leq i \leq R)$$

*has a nontrivial solution in $T_p^N$ provided that*

$$N > \sum_{i=1}^{R} k_i \frac{p^{v_i} - 1}{p - 1}.$$

Our next lemma is a version of Hensel's Lemma, which allows us to lift a nonsingular solution of a system of congruences to a $p$-adic solution. This is Lemma 4 of [7].

LEMMA 6. *Consider the system (1). Let $p$ be a prime number, and for $1 \le i \le R$ we define numbers $\tau_i$ and $\tilde{k}_i$ such that $k_i = p^{\tau_i} \tilde{k}_i$ with $(p, \tilde{k}_i) = 1$. Further, for $1 \le i \le R$, we define*

$$\gamma_i = \begin{cases} \tau_i & \text{if } p \text{ is odd} \\ \tau_i + 1 & \text{if } p = 2. \end{cases}$$

*Let $h$ be a positive integer and suppose that $\mathbf{z}$ is a nontrivial solution of the system of congruences*

$$F_i(\mathbf{x}) \equiv 0 \pmod{p^{2h+\gamma_i-1}} \qquad (1 \le i \le R) \tag{6}$$

*such that the matrix*

$$\begin{bmatrix} a_{11} z_1^{k_1-1} & \cdots & a_{1s} z_s^{k_1-1} \\ \vdots & & \vdots \\ a_{R1} z_1^{k_R-1} & \cdots & a_{Rs} z_s^{k_R-1} \end{bmatrix} \tag{7}$$

*has an $R \times R$ submatrix $M$ such that*

$$\det M \not\equiv 0 \pmod{p^h}. \tag{8}$$

*Then the system (1) has a solution $\mathbf{y} \in \mathbb{Z}_p^s$ such that $\mathbf{y} \equiv \mathbf{z} \pmod{p^h}$.*

Our final goal for this section is to prove Lemma 10, a result stating that under certain conditions the determinant of a matrix similar to (7) can be made to be nonzero modulo a power of a prime $p$. This will be needed later to ensure that our solutions of congruences are nonsingular. In order to prove this lemma, we will need some properties of Bhargava's generalized factorial function (see [2, 3, 4]), and refer the reader to [4] for the definition of a $p$-ordering and the definitions of the functions $v_k(S,p), w_p(a)$ and $k!_S$. In order to prove Lemma 10, we will need the following preliminary lemmata.

LEMMA 7. *The sequence $0, 1, 2, \dots$ of nonnegative integers is a $p$-ordering for $\mathbb{Z}$ for any prime $p$.*

This is Proposition 6 of [4].

Lemma 8. *Let $p$ be a prime number, and let $S$ be the set $S = \mathbb{Z} - p\mathbb{Z}$. Then the sequence*

$$(a_0, a_1, a_2, \ldots) = (1, 2, 3, \ldots, p-1, p+1, \ldots, 2p-1, 2p+1, \ldots)$$

*is a p-ordering for $S$.*

**Proof.** In the definition of a $p$-ordering, we may take $a_0$ to be any element of $S$. Hence it is permissible to set $a_0 = 1$. Now suppose that $a_0, \ldots, a_k$ are the first $k+1$ terms of a $p$-ordering for $S$. We wish to show that $a_{k+1}$ is allowable for the next term. We divide the proof into two cases. First, if $p \nmid (a_k + 1)$, then $a_{k+1} = a_k + 1$. Let $mp$ be the largest multiple of $p$ such that $mp < a_k$. Suppose by way of contradiction that we cannot use $a_{k+1}$ as the next term. Then there is some number $y \in S - \{a_0, \ldots, a_k\}$ such that

$$w_p((y - a_0) \cdots (y - a_k)) < w_p((a_{k+1} - a_0) \ldots (a_{k+1} - a_k)).$$

Since any element of $S$ is relatively prime to $p$, we have

$$
w_p\left(\prod_{i=0}^{a_k}(y - i)\right) = w_p\left(\prod_{j=0}^{k}(y - a_j)\right) \cdot w_p\left(\prod_{j=0}^{m}(y - jp)\right)
$$

$$
< w_p\left(\prod_{j=0}^{k}(a_{k+1} - a_j)\right) \cdot w_p\left(\prod_{j=0}^{m}(a_{k+1} - jp)\right)
$$

$$
= w_p\left(\prod_{i=0}^{a_k}(a_{k+1} - i)\right),
$$

where the inequality holds because

$$
w_p\left(\prod_{j=0}^{m}(y - jp)\right) = w_p\left(\prod_{j=0}^{m}(a_{k+1} - jp)\right) = 1
$$

since $a_{k+1}$ and $y$ are both relatively prime to $p$. However we cannot have an element $y \in S - \{a_0, \ldots, a_k\}$ such that

$$
w_p\left(\prod_{i=0}^{a_k}(y - i)\right) < w_p\left(\prod_{i=0}^{a_k}(a_{k+1} - i)\right)
$$

11

since then the sequence $0, 1, 2, \ldots$ would not be a valid $p$-ordering of $\mathbb{Z}$, contradicting Lemma 7.

Now suppose that $p \mid (a_k + 1)$, and write $a_k + 1 = mp$. Then $a_{k+1} = a_k + 2$. As before, suppose by way of contradiction that there is an element $y \in S - \{a_0, \ldots, a_k\}$ with

$$w_p((y - a_0) \cdots (y - a_k)) < w_p((a_{k+1} - a_0) \cdots (a_{k+1} - a_k)).$$

Again noting that both $y$ and $a_{k+1}$ are prime to $p$, we have

$$w_p \left( \prod_{i=0}^{a_k+1} (y - i) \right) = w_p \left( \prod_{i=0}^{k} (y - a_i) \right) \cdot w_p \left( \prod_{j=0}^{m} (y - jp) \right)$$

$$< w_p \left( \prod_{i=0}^{k} (a_{k+1} - a_i) \right) \cdot w_p \left( \prod_{j=0}^{m} (a_{k+1} - jp) \right)$$

$$= w_p \left( \prod_{i=0}^{a_k+1} (a_{k+1} - i) \right),$$

and the existence of such an element $y$ again violates Lemma 7. Hence, after having chosen $a_0, \ldots, a_k$, the element $a_{k+1}$ is allowable for the next term of a $p$-ordering on $S$. So the lemma is true by induction.$\square$

LEMMA 9. *Suppose that the sequence $a_0, a_1, \ldots$ is a p-ordering for the set $S$. A polynomial $F$ of degree $k$, written in the form*

$$F(x) = \sum_{n=0}^{k} e_n (x - a_0)(x - a_1) \cdots (x - a_{n-1}),$$

*vanishes on $S$ modulo $p^r$ if and only if $e_n$ is a multiple of $p^r / (p^r, n!_S)$ for $0 \leq n \leq k$.*

This is Lemma 14 of [4].

LEMMA 10. *Consider the matrix*

$$B = \begin{bmatrix} a_{11} x_1^{k_1 - 1} & \cdots & a_{1R} x_R^{k_1 - 1} \\ \vdots & & \vdots \\ a_{R1} x_1^{k_R - 1} & \cdots & a_{RR} x_R^{k_R - 1} \end{bmatrix}, \tag{9}$$

and assume that $a_{11}a_{22}\cdots a_{RR} \not\equiv 0 \pmod{p}$. *Then the following statements hold.*

*i) If $p > k_1 - k_R + 1$, then there exist integers $t_2, \ldots, t_R$, all relatively prime to $p$, such that if we set $x_2 = t_2 x_1, \ldots, x_R = t_R x_1$ and let $x_1$ be any integer relatively prime to $p$, then $\det B \not\equiv 0 \pmod{p}$.*

*ii) If we have*

$$p > 1 + \max\left\{ k_1 - k_{R-1}, \frac{k_1 - k_R}{2} \right\},$$

*then there exist integers $t_2, \ldots, t_R$, all relatively prime to $p$, such that if we set $x_2 = t_2 x_1, \ldots, x_R = t_R x_1$ and let $x_1$ be any integer relatively prime to $p$, then $\det B \not\equiv 0 \pmod{p^2}$.*

Note that if $R = 1$ we interpret the condition in part ii) of the lemma as $p > 1$.

**Proof.** First note that if we set $x_2 = t_2 x_1, \ldots, x_R = t_R x_1$, then we have

$$\det B = x_1^{k_1 + \cdots + k_R - R}(t_2 \cdots t_R)^{k_R - 1} \det C,$$

where $C$ is the matrix

$$C = \begin{bmatrix} a_{1,1} & a_{1,2}t_2^{k_1 - k_R} & \cdots & a_{1,R}t_R^{k_1 - k_R} \\ \vdots & \vdots & & \vdots \\ a_{R-1,1} & a_{R-1,2}t_2^{k_{R-1} - k_R} & \cdots & a_{R-1,R}t_R^{k_{R-1} - k_R} \\ a_{R,1} & a_{R,2} & \cdots & a_{R,R} \end{bmatrix}.$$

Since we require $x_1, t_2, \ldots, t_R$ to all be nonzero modulo $p$, the matrix $B$ has the desired property if and only if $\det C$ is nonzero modulo the appropriate power of $p$.

We prove part i) of the lemma by induction on $R$. If $R = 1$, then $\det B = a_{11}x_1^{k_1 - 1}$. If $a_{11}$ and $x_1$ are both relatively prime to $p$, then so is $\det B$. Now suppose that the statement is true for $R = M - 1$. We wish to prove that it holds for $R = M$. In this

situation, we have

$$B = \begin{bmatrix} a_{11}x_1^{k_1-1} & \cdots & a_{1M}x_M^{k_1-1} \\ \vdots & & \vdots \\ a_{M1}x_1^{k_M-1} & \cdots & a_{MM}x_M^{k_M-1} \end{bmatrix},$$

and the matrix $C$ becomes

$$C = \begin{bmatrix} a_{1,1} & a_{1,2}t_2^{k_1-k_M} & \cdots & a_{1,M}t_M^{k_1-k_M} \\ \vdots & \vdots & & \vdots \\ a_{M-1,1} & a_{M-1,2}t_2^{k_{M-1}-k_M} & \cdots & a_{M-1,M}t_M^{k_{M-1}-k_M} \\ a_{M,1} & a_{M,2} & \cdots & a_{M,M} \end{bmatrix}.$$

Now consider the upper left-hand $(M-1) \times (M-1)$ submatrix of $B$. By the inductive hypothesis, choose integers $t_2, \ldots, t_{M-1}$ all nonzero modulo $p$ such that the determinant of this matrix is nonzero modulo $p$ whenever $x_1$ is relatively prime to $p$. Hence the determinant of the upper left-hand $(M-1) \times (M-1)$ submatrix $D$ of $C$ is also nonzero modulo $p$. Then we have

$$C = \left[ \begin{array}{ccc|c} & & & a_{1,M}t_M^{k_1-k_M} \\ & \text{\Large $D$} & & \vdots \\ & & & a_{M-1,M}t_M^{k_{M-1}-k_M} \\ \hline a_{M,1} & a_{M,2} \quad \cdots \quad a_{M,M-1} & & a_{M,M} \end{array} \right]$$

and by expanding along the rightmost column we get

$$\det C = a_{MM} \det D + p(t_M),$$

where

$$p(t_M) = c_1 t_M^{k_1-k_M} + \cdots + c_{M-1} t_M^{k_{M-1}-k_M}$$

is a polynomial with no constant term. If $c_1, \ldots, c_{M-1}$ are all divisible by $p$, then we can set $t_M = 1$ and obtain

$$\det C \equiv a_{MM} \det D \not\equiv 0 \pmod{p}.$$

14

If some of the $c_i$ are nonzero modulo $p$, then we note that $\det C$ is a polynomial of degree at most $k_1 - k_M$. If $p - 1 > k_1 - k_M$, then $\det C$ cannot be divisible (as a polynomial) by

$$t_M^{p-1} - 1 = (t_M - 1)(t_M - 2) \cdots (t_M - (p-1)).$$

Since the ring $(\mathbb{Z}/p\mathbb{Z})[t_M]$ has unique factorization, there must be a value for $t_M$ which is nonzero modulo $p$ and for which $\det C \not\equiv 0 \pmod{p}$. Therefore the values we have chosen for $t_2, \ldots, t_M$ ensure that $\det B \not\equiv 0 \pmod{p}$ whenever $(x_1, p) = 1$. This completes the proof of part i) of the lemma.

To prove part ii), first note that if $R = 1$, then the same argument as above shows that the statement is true whenever $p > 1$. Now consider the matrix $B$ given in (9). Since $p > k_1 - k_{R-1} + 1$, we can choose values of $t_2, \ldots, t_{R-1}$ such that the upper left-hand $(R-1) \times (R-1)$ submatrix of $B$ will be nonsingular modulo $p$ whenever $(x_1, p) = 1$. As in the proof of part i), this implies that the upper left-hand $(R-1) \times (R-1)$ submatrix $D$ of $C$ will also be nonsingular modulo $p$. Thus we just need to choose a value for $t_R$.

We can now write

$$\det C = p(t_R) = c_{k_1 - k_R} t_R^{k_1 - k_R} + \cdots + c_{k_{R-1} - k_R} t_R^{k_{R-1} - k_R} + a_{RR} \det D.$$

Note that this polynomial is slightly different than the one we called $p(t_M)$ earlier. We wish to show that this polynomial does not vanish modulo $p^2$ on the set $S = \mathbb{Z} - p\mathbb{Z}$. Since $a_{RR} \det D \not\equiv 0 \pmod{p}$, this is certainly true if $c_{k_i - k_R} \equiv 0 \pmod{p}$ for $1 \leq i \leq R - 1$. If at least one of these coefficients is nonzero modulo $p$, let $d$ be the smallest number such that $c_{k_d - k_R} \not\equiv 0 \pmod{p}$.

Let $a_0, a_1, \ldots$ be the $p$-ordering for $S$ given in Lemma 8, and write $p(t_R)$ in the form

$$p(t_R) = \sum_{n=0}^{k_1 - k_R} e_n (t_R - a_0) \cdots (t_R - a_{n-1}), \tag{10}$$

as in Lemma 9. Note that because of the way we chose $d$, we have $p \mid e_n$ whenever

15

$n > k_d - k_R$. It is then not too hard to see that we must have

$$e_{k_d - k_R} \equiv c_{k_d - k_R} \not\equiv 0 \pmod{p}.$$

We now show that if $p > 1 + (k_1 - k_R)/2$, then $e_{k_d - k_R}$ is not a multiple of

$$\frac{p^2}{(p^2, (k_d - k_R)!_S)}.$$

Once this is done, our proof will be complete by Lemma 9.

In order to prove this divisibility criterion, we examine the values of $p^2/(p^2, n!_S)$. First note that we have

$$n!_S = \prod_{q \text{ prime}} v_n(S, q)$$

and that $v_n(S, q)$ is a power of $q$. (Again, see [4] for an elementary explanation of Bhargava's factorial function and this notation.) Since $p$ is prime, the terms $v_n(S, q)$ with $q \neq p$ do not contribute anything to $(p^2, n!_S)$ and so we have

$$(p^2, n!_S) = (p^2, v_n(S, p)).$$

By simply writing out the terms $a_0, a_1, \ldots$ for the $p$-ordering for $S$ given in Lemma 8, it is easy to see that

$$v_n(S, p) = \begin{cases} 1 & \text{if} & n \leq p - 2 \\ p & \text{if} & p - 1 \leq n \leq 2p - 3 \\ p^2 L_n, \ L_n \in \mathbb{Z} & \text{if} & n \geq 2p - 2. \end{cases}$$

Hence we see that

$$\frac{p^2}{(p^2, n!_S)} = \frac{p^2}{(p^2, v_n(S, p))} = \begin{cases} p^2 & \text{if} & n \leq p - 2 \\ p & \text{if} & p - 1 \leq n \leq 2p - 3 \\ 1 & \text{if} & n \geq 2p - 2. \end{cases}$$

Note that if $p > 1 + (k_1 - k_R)/2$, then $k_1 - k_R \leq 2p - 3$. Since $k_d - k_R \leq k_1 - k_R$, this implies that

$$\frac{p^2}{(p^2, (k_d - k_R)!_S)} = p \ \text{or} \ p^2.$$

But this number cannot divide $e_{k_d - k_R}$ since $e_{k_d - k_R}$ is nonzero modulo $p$. This completes the proof of the lemma. $\square$

# 4. The Proof of Theorem 2

Since the proofs of the first bound in both parts of Theorem 2 are essentially identical, we prove them together. In what follows, setting $m = 1$ proves the first bound in part i) of the theorem and setting $m = 2$ proves the first bound in part ii). We remark first that if there is some number $N$ such that any system like (1) in $N$ variables has a nontrivial $p$-adic solution, then any such system in $s > N$ variables also has one. This can be seen by simply setting $s - N$ of the variables equal to zero, leaving a system in $N$ variables. It therefore suffices to assume that we have

$$s = (S_m + 1) \sum_{i=1}^{R} ik_i - \sum_{i=1}^{R} k_i + R$$

variables and show that the system (1) has a nontrivial $p$-adic solution.

Since it is enough to prove each part of the theorem for $p$-normalized systems of forms, we will assume throughout this section that all systems are $p$-normalized. However, we must define the quantities $r$ and $|M_1|, \ldots, |M_R|$ used in the normalization process. To do this, we set $r = R$ and

$$|M_i| = ik_i(S_m + 1) - k_i \quad (1 \leq i \leq R).$$

For each $i$, Lemma 4 yields

$$q_i \geq \left( |M_i| + \frac{r}{R} \right) \frac{1}{k_i}$$
$$= i(S_m + 1) - 1 + \frac{1}{k_i}.$$

But since $q_i$ must be an integer, this implies that we have $q_i \geq i(S_m + 1)$. In other words, for each $i$ the form $F_i$ of degree $k_i$ contains at least $i(S_m + 1)$ variables which are explicit when $F_i$ is reduced modulo $p$.

We now relabel the variables in our system using the following procedure. Since $q_1 \geq S_m + 1$, we can choose $S_m + 1$ variables which are explicit when $F_1$ is reduced

modulo $p$. Let $\mathfrak{U}_1$ be the set containing these variables. Since $q_2 \geq 2(S_m + 1)$, we can choose a set $\mathfrak{U}_2$ containing $S_m + 1$ variables which are explicit when $F_2$ is reduced modulo $p$ and which are not in $\mathfrak{U}_1$. We can continue this procedure to define sets $\mathfrak{U}_3, \ldots, \mathfrak{U}_R$, where each $\mathfrak{U}_i$ contains $S_m + 1$ variables, all of which are explicit when $F_i$ is considered modulo $p$, such that $\mathfrak{U}_1, \ldots, \mathfrak{U}_R$ are pairwise disjoint. We now relabel the variables in such a manner that for each $i$, the variables in the set $\mathfrak{U}_i$ are labeled

$$x_i, x_{R+i}, \ldots, x_{RS_m+i}.$$

If $i > R(S_m + 1)$, then we set $x_i = 0$. This leaves us with a system

$$
\begin{array}{ccccccc}
F_1(\mathbf{x}) & = & a_{1,1}x_1^{k_1} & + \cdots + & a_{1,R(S_m+1)}x_{R(S_m+1)}^{k_1} & = & 0 \\
\vdots & & \vdots & & \vdots & & \vdots \\
F_R(\mathbf{x}) & = & a_{R,1}x_1^{k_R} & + \cdots + & a_{R,R(S_m+1)}x_{R(S_m+1)}^{k_R} & = & 0,
\end{array}
\tag{11}
$$

which has the property that for $0 \leq j \leq S_m$, we have

$$a_{1,jR+1}a_{2,jR+2}\cdots a_{R,jR+R} \not\equiv 0 \pmod{p}.$$

In other words, if we let $A_1$ be the matrix of coefficients of the first $R$ variables, $A_2$ be the matrix of coefficients of the second $R$ variables, and so on, then each diagonal element of each of these matrices is nonzero modulo $p$.

To find a $\mathbb{Q}_p$-integral solution to (11), we will first find a solution of the system

$$
\begin{array}{ccc}
a_{1,1}x_1^{k_1} + \cdots + a_{1,R(S_m+1)}x_{R(S_m+1)}^{k_1} \equiv 0 & \pmod{p^{2m+\tau_1-1}} \\
\vdots \qquad\qquad \vdots \qquad\qquad \vdots & \\
a_{R,1}x_1^{k_R} + \cdots + a_{R,R(S_m+1)}x_{R(S_m+1)}^{k_R} \equiv 0 & \pmod{p^{2m+\tau_R-1}}
\end{array}
\tag{12}
$$

which is nonsingular modulo $p^m$, where we recall that each $\tau_i$ is defined so that $k_i = p^{\tau_i}\tilde{k}_i$ with $(p, \tilde{k}_i) = 1$. Note that since both parts of the theorem require $p$ to be odd, the powers of $p$ in (12) are the powers required in Lemma 6 when $h = m$.

If the bounds on $p$ given in the statement of the theorem hold, then Lemma 10 tells us that for each $j$ with $0 \leq j \leq S_m$, we can find integers $t_{jR+2}, \ldots, t_{jR+R}$ such that if we set

$$x_{jR+i} = t_{jR+i}x_{jR+1}, \qquad (2 \leq i \leq R)$$

and let $B_j$ be the matrix

$$B_j = \begin{bmatrix} a_{1,jR+1}x_{jR+1}^{k_1-1} & \cdots & a_{1,jR+R}x_{jR+R}^{k_1-1} \\ \vdots & & \vdots \\ a_{R,jR+1}x_{jR+1}^{k_R-1} & \cdots & a_{R,jR+R}x_{jR+R}^{k_R-1} \end{bmatrix},$$

then we have $\det B_j \not\equiv 0 \pmod{p^m}$ whenever $x_{jR+1} \not\equiv 0 \pmod{p}$.

After making the identifications above, we obtain a new system

$$c_{1,1}x_1^{k_1} + c_{1,R+1}x_{R+1}^{k_1} + \cdots + c_{1,RS_m+1}x_{RS_m+1}^{k_1} \equiv 0 \pmod{p^{2m+\tau_1-1}}$$
$$\vdots \qquad\qquad \vdots \qquad\qquad\qquad \vdots \qquad\qquad\qquad \vdots \qquad\qquad\qquad (13)$$
$$c_{R,1}x_1^{k_R} + c_{R,R+1}x_{R+1}^{k_R} + \cdots + c_{R,RS_m+1}x_{RS_m+1}^{k_R} \equiv 0 \pmod{p^{2m+\tau_R-1}}.$$

Suppose that we can find a solution to this system with at least one of the variables, say $x_{jR+1}$, not divisible by $p$. This would lead to a solution of the system (12) in which the matrix $B_j$ satisfies $\det B_j \not\equiv 0 \pmod{p^m}$. Then the solution of (12) lifts to a nontrivial solution of (11) by Lemma 6, and this gives us a nontrivial solution of (1). Thus it suffices to show that the system (13) has a nontrivial solution.

We find a nontrivial solution of (13) with the variables restricted to the Teichmüller set $T_p = \{x \in \mathbb{Z}_p : x^p = x\}$. Note that when $x \in T_p$, we have

$$x^{k_i} = x^{p^{\tau_i}\tilde{k}_i} = x^{\tilde{k}_i}.$$

Therefore any solution of the system

$$c_{1,1}x_1^{\tilde{k}_1} + c_{1,R+1}x_{R+1}^{\tilde{k}_1} + \cdots + c_{1,RS_m+1}x_{RS_m+1}^{\tilde{k}_1} \equiv 0 \pmod{p^{2m+\tau_1-1}}$$
$$\vdots \qquad\qquad\qquad \vdots \qquad\qquad\qquad \vdots \qquad\qquad\qquad (14)$$
$$c_{R,1}x_1^{\tilde{k}_R} + c_{R,R+1}x_{R+1}^{\tilde{k}_R} + \cdots + c_{R,RS_m+1}x_{RS_m+1}^{\tilde{k}_R} \equiv 0 \pmod{p^{2m+\tau_R-1}}$$

19

with all the variables in $T_p$ is also a solution of (13). By Lemma 5, we can solve (14) nontrivially whenever the number of variables is greater than

$$\sum_{i=1}^{R} \tilde{k}_i \frac{p^{2m+\tau_i-1}-1}{p-1} = S_m.$$

Since we have $S_m + 1$ variables, there exists a nontrivial solution to (14) with each variable in $T_p$. As mentioned above, this is also a nontrivial solution of (13), and this leads to a nontrivial solution of (1). The first bound in each part of the theorem follows.

To finish the proof, we need to show that the second bound in each part of the theorem holds. For part i), note that we have

$$S_1 = \sum_{i=1}^{R} \tilde{k}_i \frac{p^{\tau_i+1}-1}{p-1} = \frac{p}{p-1} \sum_{i=1}^{R} k_i - \sum_{i=1}^{R} \frac{\tilde{k}_i}{p-1}.$$

Since $p \geq 3$, we obtain

$$S_1 + 1 < 1 + \frac{p}{p-1} \sum_{i=1}^{R} k_i$$

$$\leq 1 + \frac{3}{2} \sum_{i=1}^{R} k_i,$$

and since $i \leq R$, we have

$$\sum_{i=1}^{R} i k_i \leq R \sum_{i=1}^{R} k_i.$$

From the first bound in part i), we then find that

$$\Gamma_p^*(k_1, \ldots, k_R) \leq \frac{3}{2} R \left( \sum_{i=1}^{R} k_i \right)^2 + (R-1) \left( \sum_{i=1}^{R} k_i \right) + R,$$

as desired. For part ii), note that if we have

$$p > k_1 - k_R + 1,$$

then part i) of the theorem applies and yields a smaller bound than given in part ii). Hence we may assume that

$$p \leq k_1 - k_R + 1.$$

Then since we are assuming that $p \geq 3$, we have

$$
\begin{aligned}
S_2 + 1 &= 1 + \sum_{i=1}^{R} \tilde{k}_i \frac{p^{\tau_i + 3} - 1}{p - 1} \\
&< 1 + \sum_{i=1}^{R} \frac{\tilde{k}_i p^{\tau_i + 3}}{p - 1} \\
&= 1 + \frac{p}{p-1} p^2 \sum_{i=1}^{R} k_i \\
&\leq 1 + \frac{3}{2}(k_1 - k_R + 1)^2 \sum_{i=1}^{R} k_i.
\end{aligned}
$$

Therefore we obtain

$$
\begin{aligned}
(S_2 + 1) \sum_{i=1}^{R} i k_i &< \left( 1 + \frac{3}{2}(k_1 - k_R + 1)^2 \sum_{i=1}^{R} k_i \right) \sum_{i=1}^{R} R k_i \\
&= \frac{3}{2} R(k_1 - k_R + 1)^2 \left( \sum_{i=1}^{R} k_i \right)^2 + R \left( \sum_{i=1}^{R} k_i \right),
\end{aligned}
$$

and the second bound in part ii) of the theorem follows easily. This completes the proof of the theorem.$\square$

## References

[1] J. Ax and S. Kochen, "'Diophantine problems over local fields I'", *Amer. J. Math.* **87** (1965), 605–630.

[2] M. Bhargava, "'$P$-orderings and polynomial functions on arbitrary subsets of Dedekind rings'", *J. reine angew. Math.* **490** (1997), 101–127.

[3] ———, "'Generalized factorials and fixed divisors over subsets of a Dedekind domain'", *J. Number Theory* **72** (1998), 67–75.

[4] ———, "'The factorial function and generalizations'", *Amer. Math. Monthly* **107** (2000), 783–799.

[5] H. Davenport and D. J. Lewis, "'Homogeneous additive equations'", *Proc. Royal Soc. London Ser. A* **274** (1963), 443–460.

[6] ———, "'Simultaneous equations of additive type'", *R. Soc. Lond. Proc. Ser. A Math. Phys. Eng. Sci.* **264** (1969), 557–595.

[7]  M. Knapp, "'Diagonal equations of different degrees over $p$-adic fields"', *(submitted)* .

[8]  D. J. Lewis and H. L. Montgomery, "'On zeros of p-adic forms"', *Michigan Math J.* **30** (1983), 83–87.

[9]  S. H. Schanuel, "'An extension of Chevalley's theorem to congruences modulo prime powers"', *J. Number Theory* **6** (1974), 284–290.

[10]  T. D. Wooley, "'On simultaneous additive equations III"', *Mathematika* **37** (1990), 85–96.

[11]  ——, "'On simultaneous additive equations I"', *Proc. London Math. Soc. (3)* **63** (1991), 1–34.

Mathematical Sciences Department

Loyola College

4501 North Charles Street

Baltimore, MD 21210-2699

USA