

Pairs of Additive Forms of Odd Degrees

Michael P. Knapp

1. INTRODUCTION.

A special case of a conjecture commonly attributed to Emil Artin [1] states that if we consider a system of two additive homogeneous equations

$$(1) \quad \begin{aligned} a_1x_1^k + a_2x_2^k + \cdots + a_sx_s^k &= 0 \\ b_1x_1^n + b_2x_2^n + \cdots + b_sx_s^n &= 0, \end{aligned}$$

with all coefficients in \mathbb{Q} and with $s \geq k^2 + n^2 + 1$, then this system should have a nontrivial solution in p -adic integers for each prime p . That is, the system should have a solution with at least one variable not equal to zero. By work of Brauer [3], it is known that there exists a finite bound on s in terms of k and n which guarantees nontrivial

2010 *Mathematics Subject Classification.* 11D72 (primary), 11D88, 11E76 (secondary).

Key words and phrases: Forms in many variables, Artin's conjecture, Forms of odd degrees.

solutions, so the only question is whether the conjectured bound suffices. The purpose of this paper is to prove that the conjectured bound does suffice when the degrees k and n are both odd.

In order to describe the previous work on this problem, we introduce a small amount of notation. For each prime p , we write $\Gamma_p^*(k, n)$ for the smallest value of s which guarantees that the system (1) with coefficients in \mathbb{Q} will have a nontrivial p -adic solution regardless of the values of those coefficients. Further, we define

$$\Gamma^*(k, n) = \max_{p \text{ prime}} \Gamma_p^*(k, n).$$

Also, for any field \mathbb{K} , we define $\Gamma^*(k, n, \mathbb{K})$ to be the smallest s guaranteeing that if the coefficients of (1) lie in \mathbb{K} , then the system must have a nontrivial solution with variables in \mathbb{K} . Note that we have $\Gamma_p^*(k, n) \leq \Gamma^*(k, n, \mathbb{Q}_p)$ and

$$\Gamma^*(k, n) \leq \max_{p \text{ prime}} \Gamma^*(k, n, \mathbb{Q}_p).$$

We will occasionally use implicitly the obvious facts that $\Gamma_p^*(k, n) = \Gamma_p^*(n, k)$ for each prime p and that $\Gamma^*(k, n) = \Gamma^*(n, k)$.

With this notation, the aforementioned result of Brauer shows that $\Gamma^*(k, n)$ exists for each pair of degrees, and Artin's conjecture can be

restated as claiming that one always has $\Gamma^*(k, n) \leq k^2 + n^2 + 1$. If we only have one homogeneous additive equation of degree k , then we define $\Gamma_p^*(k)$, $\Gamma^*(k)$, and $\Gamma^*(k, \mathbb{K})$ similarly. Davenport & Lewis [7] have shown that $\Gamma^*(k) \leq k^2 + 1$ for all k , with equality whenever $k + 1$ is prime, confirming another special case of Artin's conjecture.

One typically bounds functions such as $\Gamma^*(k, n)$ or $\Gamma^*(k)$ by obtaining a bound on $\Gamma^*(k, n, \mathbb{Q}_p)$ in terms of p , and then finding the maximum of this bound. As a consequence of this, it is not important in the proofs of any of the bounds mentioned in this article that the coefficients are rational. All of these bounds apply to (systems of) equations in which the coefficients may be any elements of \mathbb{Q}_p .

Most previous work on the problem with two equations has dealt with the situation when both of the forms have the same degree. If the degrees are equal and odd, then Davenport & Lewis [8] showed that the conjecture is true. When the degrees are equal and even, Brüdern & Godinho [4] have shown that if the degree cannot be written either as $p^\tau(p - 1)$ with p prime and $\tau \geq 1$, or as $3 \cdot 2^\tau$ with $\tau \geq 1$, then the conjecture is true. Even when the degree does have one of these special shapes there are no known counterexamples, so the conjecture

could well be true for these degrees also.

When the degrees are different, much less is known. Leep & Schmidt [13] have proven that $\Gamma^*(k, n) \leq (k^2 + 1)(n^2 + 1)$. A few years ago, the author proved [12] that $\Gamma^*(k, n) < 64(k + 2n)(k + n)(k - n)^2$, and also that if the degree k is odd (with no restrictions on n), then $\Gamma^*(k, n) \leq k^2 + 2n^2 + 1$. It is also trivial to show from results in the literature that $\Gamma^*(3, 1) \leq 11$. A result of Lewis [14] shows that 10 variables is sufficient for a single (not necessarily diagonal) cubic form, and the work of Leep & Schmidt [13] shows that if we add a linear form, then only one additional variable is required.

The main goal of this article is to prove the following theorem.

Theorem 1. *If k and n are both positive odd integers, then we have*
$$\Gamma^*(k, n) \leq k^2 + n^2 + 1.$$

That is, we will prove that Artin's conjecture for two additive forms is correct when the degrees of the forms are both odd. As mentioned above, we prove Theorem 1 by working with p -adic coefficients in general. Thus, Theorem 1 is a consequence of the following slightly more general theorem.

Theorem 2. *If k and n are both positive odd integers and p is prime, then $\Gamma^*(k, n, \mathbb{Q}_p) \leq k^2 + n^2 + 1$.*

The underlying idea of our proof is simple. By the result of Davenport & Lewis mentioned above, we may assume that $k \neq n$. In Section 2, we will first assume that $s \geq k^2 + n^2 + 1$, and construct a linear space of large dimension on which one of the forms is identically zero. Then we will show that the other form has a solution in this linear space. This plan involves studying the solutions of one equation at a time, and so we are led to study the values of $\Gamma^*(k)$ for k odd, and in Section 3 we will prove the following result.

Theorem 3. *Suppose that $k \geq 7$ is an odd integer. Then we have $\Gamma^*(k) \leq (k^2 + 1)/2$. Additionally, we have the following values of and bounds on $\Gamma^*(k)$:*

$$\Gamma^*(13) = 53 \qquad \Gamma^*(23) = 116$$

$$\Gamma^*(15) = 61 \qquad \Gamma^*(25) = 101$$

$$\Gamma^*(17) = 52 \qquad \Gamma^*(27) \leq 271$$

$$\Gamma^*(19) = 58 \qquad \Gamma^*(29) \leq 291.$$

$$\Gamma^*(21) = 106$$

We point out here as an aside the interesting fact that $\Gamma^*(17) < \Gamma^*(13)$. This shows that if we restrict to odd values of k , or even to prime values, then $\Gamma^*(k)$ is not an increasing function.

Our proof of Theorem 3 uses a hodgepodge of techniques. Again we proceed by studying the more general function $\Gamma^*(k, \mathbb{Q}_p)$. First, we use a theorem of Tietäväinen [16] to show that Theorem refthmc is true for all odd $k \geq 31$. For the other degrees, we use several different results from the literature (see [5] and [9]) to show that our bound is true for the majority of primes p . When there exist primes not handled by these theorems, we use a brute force computation to complete the proof. (In the later stages of our work, we discovered that the method used to effect this computation is extremely similar to that used by Bierstedt in [2].) Here we make great use of a result of Norton [15, p. 165] which gives lower bounds for the values of $\Gamma^*(k)$ for odd $k \leq 25$. In fact, it turns out that in each case, Norton's lower bound is the correct value. We note that some of our work to prove Theorem refthmc overlaps the proof of Theorem 3.1 of [10]. In this theorem, the authors study a congruence equation which we need in our proof and obtain the same result as we do, but with a few added conditions that we do

not need.

Since Theorem 3 is only valid for degrees greater than 5, we will see that the proof given in Section 2 does not quite work when one degree is 5 and the other is either 3 or 1. We will treat this case in Section 4 through a small modification of the ideas in Sections 2 and 3. To complete the proof, we need the following “folklore” result that we have seen implied in the literature and have heard in private discussions.

Result. *We have $\Gamma^*(5) = 16$. Moreover, $p = 11$ is the only prime for which 16 variables are needed. For all other primes, we have $\Gamma_p^*(5) \leq 11$.*

A brief discussion of this result is in order. This result has on occasion been attributed to J. F. Gray, but this is not entirely correct. In his dissertation, Gray [11] proves that $\Gamma_p^*(5) \leq 16$ for all $p \neq 5$, and gives an example showing that $\Gamma_{11}^*(5) = 16$. Later, S. Chowla [6] gave a brief sketch of a method to deal with the case when $p = 5$. Although Gray does give the example for $p = 11$, his work does not show (and we note that it does not claim to show) that $\Gamma_p^*(5) < 16$ for all other primes. Since we use the same method to verify this result as we use

to prove Theorem 3, we treat this result in Section 3.

1.1. Acknowledgements. Much of the research contained in this paper was done while the author was supported by NSF grant DMS-0344082. This research was completed and the paper was written while the author was enjoying the hospitality of the Universidade de Brasília while on sabbatical leave. Finally, the author would like to thank the anonymous referee for pointing out an error in the original version of this article, and also for helpful suggestions which have improved the exposition.

2. THE PROOF OF THEOREM 2

2.1. Preliminaries. In this subsection, we will record two preliminary results that are needed in the proof of Theorem 2. Then in Section 2.2 we show that Theorem 2 follows from Theorem 3 when the largest degree is at least 7.

The first lemma is due to the author, and is proved on pages 153-154 of [12], although it is not explicitly stated. This lemma will help us to deal with the case when $p = 2$.

Lemma 1. *If k is a positive odd integer, then we have $\Gamma_2^*(k, n) \leq 2n^2 + k + 1$.*

Our other lemma is Lemma 7 of [12]. We will use this lemma to help us find linear spaces of zeros of forms.

Lemma 2. *Suppose that p is an odd prime, n is a positive integer, and c_1, \dots, c_s are p -adic integers which are not divisible by p . If $s \geq n + 1$, then there exist distinct indices i and j such that c_i/c_j is a n -th power in \mathbb{Z}_p .*

In [12], it is only claimed that c_i/c_j is an n -th power in \mathbb{Q}_p , but it is easy to see that this term (and its n -th root) actually lie in \mathbb{Z}_p .

2.2. The Proof when $k \geq 7$. By the result of Davenport & Lewis mentioned in the introduction, the theorem is true if $k = n$, so we may suppose without loss of generality that $k > n$, and hence that $k \geq 7$. Assume also that we have $s \geq k^2 + n^2 + 1$.

We note first that the case $p = 2$ is trivial (even if $k < 7$) by Lemma 1. This lemma implies that the system has nontrivial 2-adic solutions whenever $s \geq 2n^2 + k + 1$. However, since $k > n$ and both numbers are odd, we have $k \geq n + 2$. This implies that $k(k - 1) > n^2$, and this

immediately implies that

$$k^2 + n^2 + 1 > 2n^2 + k + 1.$$

Hence we have more than enough variables to guarantee nontrivial 2-adic solutions.

Now we turn to the case $p \geq 3$. If necessary, we multiply each equation by a constant to ensure that all of the coefficients in (1) are integers. Consider the coefficients b_1, \dots, b_s in the form of degree n . If there exist nonzero coefficients b_i such that $p^n | b_i$, then we can make a change of variables of the form $x'_i = p^{\alpha_n} x_i$ to absorb all the powers of p^n dividing b_i into the variable x_i . Thus we may assume that if $b_i \neq 0$ and $p^g | b_i$ then $0 \leq g < n$.

Now we separate the variables according to the power of p dividing their coefficients in the degree n equation. Define the set

$$V = \{i : b_i = 0\}$$

and for $0 \leq g < n$, define the sets

$$U_g = \{i : p^g \parallel b_i\}.$$

For each g , if we have $|U_g| \geq n + 1$, then by Lemma 2 we can find two coefficients b_i and b_j and an element $\zeta \in \mathbb{Z}_p$ such that $b_i = \zeta^n b_j$. Hence we can solve the equation

$$(2) \quad b_i x_i^n + b_j x_j^n = 0$$

by setting $x_i = 1$ and $x_j = -\zeta$. Using Lemma 2 repeatedly, we see that we can find at least $(|U_g| - n)/2$ pairwise disjoint pairs of variables x_i, x_j such that the equation (2) has a nontrivial solution in \mathbb{Z}_p . Therefore, after possibly relabeling variables, we can rewrite the degree n equation in (1) as

$$\begin{aligned} & b_1 x_1^n + b_2 x_2^n + \cdots + b_{2N-1} x_{2N-1}^n + b_{2N} x_{2N}^n \\ & + b_{2N+1} x_{2N+1}^n + \cdots + b_{2N+|V|} x_{2N+|V|}^n \\ & + b_{2N+|V|+1} x_{2N+|V|+1}^n + \cdots + b_s x_s^n = 0, \end{aligned}$$

where for $i = 1, \dots, N$ there exist nonzero p -adic numbers y_{2i-1} and y_{2i} such that

$$b_{2i-1} y_{2i-1}^n + b_{2i} y_{2i}^n = 0,$$

and for $i = 2N + 1, \dots, 2N + |V|$ we have $b_i = 0$.

Next, for $i = 1, \dots, N$, we set $x_{2i-1} = y_{2i-1} Y_i$ and $x_{2i} = y_{2i} Y_i$. Also, we set $x_i = Y_{i-N}$ when $2N + 1 \leq i \leq 2N + |V|$ and set $x_i = 0$ when

$i > 2N + |V|$. Then we see that the degree n equation in (1) is satisfied for any choice of $Y_1, \dots, Y_{N+|V|}$, and that if at least one of the Y_i is nonzero then we have a nontrivial solution of this equation.

After assigning the variables in this manner, the degree k equation in (1) becomes

$$(3) \quad d_1 Y_1^k + \dots + d_{N+|V|} Y_{N+|V|}^k = 0$$

for some coefficients $d_1, \dots, d_{N+|V|}$. Note that if we can solve (3) nontrivially, then this will immediately lead to a nontrivial solution of (1).

The number of variables involved in (3) is

$$\begin{aligned} N + |V| &\geq |V| + \sum_{g=0}^{n-1} \frac{|U_g| - n}{2} \\ &\geq \frac{s}{2} - \sum_{g=0}^{n-1} \frac{n}{2} \\ &\geq \frac{s}{2} - \frac{n^2}{2} \\ &\geq \frac{k^2 + 1}{2}. \end{aligned}$$

Finally, noting that (3) is a homogeneous additive equation of odd degree $k \geq 7$ in at least $(k^2 + 1)/2$ variables, we see that Theorem 3 implies that this equation has a nontrivial solution in \mathbb{Q}_p . As mentioned above, this implies that the original system (1) has a nontrivial

solution. Hence the proof of this case of Theorem 2 will be complete once Theorem 3 is established.

3. THE PROOF OF THEOREM 3

3.1. Preliminaries. The goal of this section is to prove Theorem 3. In addition to being interesting in its own right, this will complete the proof of Theorem 2 (except for the case when $k = 5$). For the majority of our work, our strategy is to bound $\Gamma_p^*(k)$ by showing that all additive forms of degree k in sufficiently many variables have a nonsingular zero modulo a suitable power of p , and then using Hensel's Lemma to lift this to a zero in \mathbb{Z}_p . We note that some of our work here overlaps with results found in [10]. There, a similar congruence result is shown, with the restrictions that the congruences are modulo p (instead of possibly modulo a power of p) and that $\gcd(k, p-1) \neq (p-1)/2$.

In order to guarantee that our forms have nonsingular zeros modulo powers of p , we must employ a normalization process which we now describe. Suppose that we have an additive form

$$(4) \quad F(\mathbf{x}) = a_1x_1^k + a_2x_2^k + \cdots + a_sx_s^k,$$

and we wish to solve the equation

$$(5) \quad F(\mathbf{x}) = a_1x_1^k + a_2x_2^k + \cdots + a_sx_s^k = 0.$$

Clearly, if $a_i=0$ for some i , then the equation (5) has a nontrivial solution. Hence we may assume that $a_i \neq 0$ for all i . Now, we say that a polynomial $G(\mathbf{x})$ is *equivalent* to $F(\mathbf{x})$ if there exists a form

$$F(l_1x_1, \dots, l_sx_s)$$

which is a (nonzero) constant multiple of G . Obviously, G has a nontrivial zero if and only if F does. We now quote a lemma of Davenport & Lewis showing that F is equivalent to a form with many coefficients nonzero modulo small powers of p . This is Lemma 3 of [7].

Lemma 3. *An additive form as in (4) is equivalent to one of the shape*

$$G = G_0 + pG_1 + \cdots + p^{k-1}G_{k-1},$$

where each G_i is an additive form in m_i variables, and each variable in each G_i has a coefficient not divisible by p , and where we also have

$$m_0 + \cdots + m_{i-1} \geq is/k$$

for $1 \leq i \leq k$.

Since $s \geq (k^2 + 1)/2$, this implies that we have $m_0 \geq (k + 1)/2$ and $m_0 + m_1 \geq k + 1$.

As stated above, our goal is to solve the equation (5) modulo a suitable power of p , and then lift the solution to a solution in \mathbb{Z}_p . We now state a version of Hensel's Lemma which allows us to do this.

Lemma 4. *Suppose that $p^\tau \parallel k$, and define $\gamma = \gamma(k, p)$ by*

$$\gamma = \begin{cases} 1 & \text{if } \tau = 0 \\ \tau + 1 & \text{if } \tau > 0 \text{ and } p > 2 \\ \tau + 2 & \text{if } \tau > 0 \text{ and } p = 2. \end{cases}$$

Consider a congruence of the form

$$(6) \quad a_1 x_1^k + \cdots + a_t x_t^k \equiv 0 \pmod{p^\gamma}.$$

If this equation has a solution such that at least one variable not divisible by p has a coefficient not divisible by p , then this solution lifts to a nontrivial solution in \mathbb{Q}_p .

We will refer to a solution of (6) of the type described in the Lemma as a *nonsingular* solution. When we use this lemma, we will typically assume that none of the coefficients are divisible by p , so that any solution with any variable not divisible by p is nonsingular.

We now state three results which we will use to guarantee that certain congruences have nonsingular solutions. The first of these is due to Dodson [9], and will be used for small primes.

Lemma 5. *Suppose that -1 is a k -th power residue modulo p^γ . Then the congruence (6), with all coefficients not divisible by p , has a nonsingular solution whenever we have $2^t > p^\gamma$.*

Our second lemma for solving congruences also can be found in [9]. While it is not explicitly stated as a lemma, the result appears (in a slightly different form) in the proof of Lemma 2.4.1 of [9].

Lemma 6. *The congruence*

$$a_1x_1^k + \cdots + a_tx_t^k \equiv 0 \pmod{p},$$

with all coefficients not divisible by p , has a nonsingular solution whenever we have

$$p > (d - 1)^{(2t-2)/(t-2)},$$

where $d = (k, p - 1)$.

Our last lemma about congruences is the well-known Chevalley's theorem [5]. While this theorem can of course be extended to systems of equations of any degrees, we only state it in a form that we need.

Lemma 7. *Suppose that $f(x_1, \dots, x_t)$ is a polynomial of (total) degree d with no constant term over a finite field \mathbb{F}_p . If $t > d$, then the equation $f(\mathbf{x}) = 0$ has a nontrivial solution in \mathbb{F}_p .*

The next lemma is due to Tietäväinen [16]. Although this lemma is not explicitly stated in [16], it is obvious that Tietäväinen wants the reader to infer this result from his Lemma 3 and the remarks preceding that lemma.

Lemma 8. *If k is odd, then we have $\Gamma^*(k) \leq 1 + k(t - 1)$, where t is the smallest number satisfying*

$$(7) \quad 2^{t-3} \geq t^2 k.$$

This definition of t guarantees that for all primes p , the congruence (6) has a nonsingular solution. It is well-known that

$$\Gamma^*(k) \leq 1 + k(t - 1)$$

for any t with this property (see for example Lemma 6.4 of [15] or Lemma 4.2.1 of [9]). Tietäväinen's contribution was to show that we can take t as in (7). We note for later use that the above formula can be slightly extended. If t_p represents a number of variables which guarantees that (6) has a nonsingular solution for a fixed prime p , then

we have

$$\Gamma_p^*(k) \leq 1 + k(t_p - 1).$$

Our final lemma is due to Norton [15]. For the degrees for which we are evaluating $\Gamma^*(k)$ exactly, this lemma shows that our proposed values are lower bounds for this function.

Lemma 9. *The following values of $\Gamma^*(k)$ hold:*

$$\Gamma^*(13) = 53 \text{ or } 66$$

$$\Gamma^*(15) = 61, 76, \text{ or } 91$$

$$\Gamma^*(17) = 52, 69, 86, \text{ or } 103$$

$$\Gamma^*(19) = 58, 77, 96, \text{ or } 115$$

$$\Gamma^*(21) = 106, 127, \text{ or } 148$$

$$\Gamma^*(23) = 116, 139, \text{ or } 162$$

$$\Gamma^*(25) = 101, 126, 151, \text{ or } 176.$$

3.2. The proof when $k \geq 31$. When $k \geq 31$, the proof of Theorem 3 is a trivial corollary of Lemma 8. It is not hard to see that if $k \geq 31$ then the number t defined in (7) is at most $(k+1)/2$. One then immediately finds that

$$\Gamma^*(k) \leq 1 + k \left(\frac{k+1}{2} - 1 \right) < \frac{k^2 + 1}{2}.$$

This completes the proof for large values of k . We note that this bound is not best possible for large odd k . In fact, the main theorem of [16] is that

$$\limsup_{\substack{k \rightarrow \infty \\ k \text{ odd}}} \frac{\Gamma^*(k)}{k \log k} = \frac{1}{\log 2}.$$

Thus, for large odd degrees, $\Gamma^*(k)$ is much smaller than the bound in Theorem 3.

3.3. The proof when $k \leq 29$. For the remaining cases, Tietäväinen's bound does not suffice for our purposes, and so we use other methods instead. The values $\Gamma^*(7) = 22$ and $\Gamma^*(11) = 45$ appear to have first been given by Bierstedt [2]. These values were independently discovered by Norton [15], who also gave the value $\Gamma^*(9) = 37$. Dodson also discovered independently the values of $\Gamma^*(7)$ and $\Gamma^*(9)$, stating in [9] that these values can be determined using the results of that paper, although he does not give a proof.

For each k , write $s(k)$ for our proposed value of (or bound on) $\Gamma^*(k)$. Note that the bounds claimed for $\Gamma^*(27)$ and $\Gamma^*(29)$ are smaller than $(27^2 + 1)/2$ and $(29^2 + 1)/2$, respectively. Lemma 9 shows that these are lower bounds when $k \leq 25$, so we only need to show that $\Gamma^*(k) \leq s(k)$ for each k . By Lemma 3, we may assume that for each degree, there

are at least $t(k) = \lceil s(k)/k \rceil$ variables in our form whose coefficients are not divisible by k . Suppose without loss of generality that these variables are $x_1, \dots, x_{t(k)}$, and consider the congruence (6), using only these variables. According to Lemma 4, if we can solve this congruence with at least one variable not divisible by p , then we can lift this solution to a nontrivial p -adic solution of (5).

Suppose for now that $k = 29$. With $t(29) = 11$, Lemma 5 shows that we can solve the congruence (6) whenever we have $2^{11} > p^\gamma$. We have $\gamma = 1$ for all primes except $p = 29$, when we have $\gamma = 2$, and so we can see that there are nontrivial p -adic solutions of (5) for all $p < 2048$. Next we use Lemma 6 to show that we can find p -adic solutions of (5) for all sufficiently large p . For $p > 29$, we only need to have solutions for congruences modulo p , as in the statement of the lemma. With $t(29) = 11$, Lemma 6 tells us that the congruence (6) has a nontrivial solution whenever $p > 1644$, and hence Lemma 4, along with the relation $\Gamma^*(k) \leq 1 + k(t - 1)$ (see Lemma 8 and the remarks following this lemma) says that the equation (5) has nontrivial p -adic solutions for these primes. If we apply this reasoning to all the degrees under consideration, we obtain the results in the table below. Since we

will need it later, we also include information for $k = 5$, with $s(5) = 11$.

k	$t(k)$	We have $\Gamma_p^*(k) \leq s(k)$ when
5	3	$\gamma = 1$ and either $p < 8$ or $p > 256$
13	5	$\gamma = 1$ and either $p < 32$ or $p > 754$
15	5	either $p < 32$ or $p > 1138$
17	4	either $p < 16$ or $p > 4096$
19	4	either $p < 16$ or $p > 5382$
21	6	either $p < 64$ or $p > 1788$
23	6	$\gamma = 1$ and either $p < 64$ or $p > 2270$
25	5	$\gamma = 1$ and either $p < 32$ or $p > 4792$
27	11	all values of p
29	11	all values of p

For $k = 27$ and $k = 29$, we have $\Gamma_p^*(k) \leq s(k)$ for all primes, and so for these degrees the proof is complete.

We can deal with many of the remaining primes without using a brute force computation. Consider the pairs of k and p for which $\gamma = 1$ and $p \not\equiv 1 \pmod{k}$, and note that for these pairs we have $(k, p-1) < k$.

We can handle most of these situations easily. The key observation is

that if we write $d = (k, p - 1)$, then the set of d -th powers modulo p is the same as the set of k -th powers modulo p . Hence, instead of solving the congruence (6), we may solve the congruence

$$(8) \quad a_1 x_1^d + \cdots + a_t x_t^d \equiv 0 \pmod{p^\gamma}$$

instead. If it happens that $d = 1$ or $d = 3$, then by Lemma 7, we can solve (8) nontrivially whenever $t \geq d + 1$. Since this is the case for every value of k we are considering, the proof is complete in these cases.

If we are in any other situation - that is, if $\gamma \geq 2$ or if $\gamma = 1$ and $(k, p - 1) \notin \{1, 3\}$ - then we show computationally that nontrivial p -adic solutions always exist. We note that in any remaining situation where $\gamma \geq 2$, we have $k = p^\tau$. In this case, we need to solve congruences modulo powers of p , and so we note that the sets of k -th powers modulo p^γ and $(\phi(p^\gamma), k)$ -th powers modulo p^γ are identical. But since $k = p^\tau$, we now have $(\phi(p^\gamma), k) = k$, and the exponent in (6) cannot be reduced. Therefore we set $d = k$ in (8), so that (8) and (6) are identical.

Once again, for a fixed prime p and odd degree k , we wish to show computationally that the congruence (8), where each coefficient is nonzero modulo p , has a nonsingular solution for each possible choice

of coefficients. To limit the computing time required, we would like to reduce the number of congruences for which we need to compute solutions. Our method for doing this is very similar to that used by Bierstedt [2]. Observe that by dividing the entire congruence by a_1 , we may assume that $a_1 \equiv 1 \pmod{p^\gamma}$. Next, note that as in Section 2.2, if we can write $a_i \equiv \zeta^d a_j \pmod{p^\gamma}$ for some indices i, j , then we can get a nonsingular solution of (8) by setting $x_i = 1, x_j = -\zeta$, and all other variables equal to 0. Hence we may assume that all of the coefficients of (8) are in different cosets of $(\mathbb{Z}/p^\gamma\mathbb{Z})^\times / (\mathbb{Z}/p^\gamma\mathbb{Z})^{\times d}$.

Moreover, suppose that (8) has a nonsingular solution for some specific choice of coefficients, and let c_i, ζ_i be numbers nonzero modulo p such that

$$c_i \equiv \zeta_i^d \cdot a_i \pmod{p^\gamma}, \quad (1 \leq i \leq t).$$

Then we can see that the congruence

$$c_1 y_1^d + \cdots + c_t y_t^d \equiv 0 \pmod{p^\gamma}$$

has a nonsingular solution by simply setting $y_i \equiv x_i / \zeta_i \pmod{p^\gamma}$.

Hence, for each coset of $(\mathbb{Z}/p^\gamma\mathbb{Z})^\times / (\mathbb{Z}/p^\gamma\mathbb{Z})^{\times d}$, we may pick one representative in $(\mathbb{Z}/p^\gamma\mathbb{Z})^\times$ and assume that it is the only element of this

coset which may appear in (8) as a coefficient.

In light of these observations, we use the following strategy in our calculations. Noting that $(\mathbb{Z}/p^\gamma\mathbb{Z})^\times/(\mathbb{Z}/p^\gamma\mathbb{Z})^{\times d}$ is cyclic, we first find a number g such that the set $\{1, g, g^2, \dots, g^{d-1}\}$ contains one representative of each coset of $(\mathbb{Z}/p^\gamma\mathbb{Z})^\times/(\mathbb{Z}/p^\gamma\mathbb{Z})^{\times d}$. Hence we may assume that $a_1 = 1$ and that $(a_2, \dots, a_t) = (g^{c_2}, \dots, g^{c_t})$, where we have $1 \leq c_2 < c_3 < \dots < c_t \leq d - 1$. This greatly reduces the number of congruences that need to be solved. Each of these congruences is solved by a brute-force approach, systematically testing each possible combination of d -th powers until a solution is found. We save some computational time by making a list of the d -th powers modulo p^γ in advance so that we don't have to repeatedly compute x_i^d for each possible choice of each variable. When these computations were completed, we found that in each case except $k = 25, p = 5$ and $k = 5, p = 5, 11$, the number of variables guaranteed to have coefficients not divisible by p was sufficient to guarantee that the congruence (8) has a nontrivial solution.

If we have $k = 25$ and $p = 5$, then it turns out that there are 10 choices of (c_2, \dots, c_5) for which the equation (8) has no nontrivial solutions. Fortunately, the normalization process tells us that we have at least 9 variables whose coefficients are not divisible by 25. To each set of coefficients for which we did not obtain solutions previously, we added one more variable, whose coefficient may or may not be divisible by 5, but is nonzero modulo 25. We then found computationally that for any possible coefficient (modulo 125) of this new variable, the congruence (8) did have nontrivial solutions. Moreover, there was always a solution in which at least one nonzero variable had a coefficient not divisible by 5. Hence, even in these “bad” cases, we are still able to guarantee that (5) has nontrivial 5-adic solutions. This completes the proof of Theorem 3.

Although it is not needed for the proof of Theorem 3, we now complete the proof of the “folklore” result mentioned in the introduction. If $k = 5$ and $p = 11$, the computer check reveals that there are essentially three congruences of the shape (6) with $t = 3$ which have no nontrivial solutions, where by “essentially” we mean that every congruence of this form with no solutions can be obtained by a combination of multiplying the entire equation by a constant and multiplying coefficients by fifth

powers. These congruences are

$$x_1^5 + 2x_2^5 + 4x_3^5 \equiv 0 \pmod{11}$$

$$x_1^5 + 2x_2^5 + 5x_3^5 \equiv 0 \pmod{11}$$

$$x_1^5 + 5x_2^5 + 8x_3^5 \equiv 0 \pmod{11}.$$

The first of these exceptional congruences is the one found by Gray [11]. We believe that the other two are new. If we add one more variable with coefficient not divisible by 11 to any of these forms, then the resulting congruence does have nontrivial solutions. This yields $\Gamma_{11}^*(5) = 16$.

For the prime $p = 5$, a brute-force computation shows that if we have three variables whose coefficients are not divisible by 5, and one additional variable whose coefficient is nonzero modulo 25 (and may or may not be divisible by 5), then the congruence (6) has solutions regardless of the coefficients. Normalization guarantees that these variables exist whenever $s \geq 11$, and hence this gives us $\Gamma_5^*(5) \leq 11$. Thus we have verified that $\Gamma^*(5) = 16$ and shown computationally that $\Gamma_p^*(5) \leq 11$ for all primes except $p = 11$.

4. THE PROOF OF THEOREM 2 WHEN $k = 5$

We now complete the proof of Theorem 2 by treating the remaining cases. As mentioned in the introduction, the case $k = 3$ is already essentially done in the literature, so we only need to treat the case $k = 5$. We will use essentially the same strategy as in Section 2.2, except that we will now treat different primes separately. Note that for a particular prime p , the proof given in Section 2.2 works as long as we have either $\Gamma_p^*(k) \leq (k^2 + 1)/2$ or $\Gamma_p^*(n) \leq (n^2 + 1)/2$. Since we have shown in Section 3.3 that $\Gamma_p^*(5) < (5^2 + 1)/2$ whenever $p \neq 11$, the theorem is true for these primes.

When $p = 11$, we deal with the case $n = 3$ through the following lemma. While the result is well-known, we cannot recall seeing it in print before, and therefore give a proof.

Lemma 10. *Let k be a positive integer, and suppose that p is a prime with $p \nmid k$ and $(k, p - 1) = 1$. Then $\Gamma_p^*(k) = k + 1$.*

Proof. As indicated in the previous section, the hypotheses of this lemma imply that $\gamma = 1$ and that every residue modulo p is a k -th power. Hence the congruence (8) is linear, and we may therefore take

$t_p = 2$ for this prime. Thus we have

$$\Gamma_p^*(k) \leq k(t_p - 1) + 1 = k + 1$$

by the remarks following Lemma 8. To see that this is actually an equality, note that the equation

$$x_1^k + px_2^k + p^2x_3^k + \cdots + p^{k-1}x_k^k = 0$$

in k variables has no nontrivial p -adic solutions. \square

This lemma immediately gives us $\Gamma_{11}^*(3) = 4 < (3^2 + 1)/2$, completing the proof that $\Gamma^*(5, 3) \leq 35$.

Finally, when $n = 1$, consider the form of degree 5. If this form has at least two coefficients equal to 0, then we can nontrivially solve the linear form using only these variables, giving a nontrivial solution of the system. Otherwise, the form of degree 5 has at least 26 nonzero coefficients, and by Lemma 3, we may assume that there are six variables (at least) with integer coefficients not divisible by 11. Suppose that these are x_1, \dots, x_6 , and define $F_1 = a_1x_1^5 + \cdots + a_6x_6^5$ and $F_2 = a_7x_7^5 + \cdots + a_{27}x_{27}^5$. Since none of the coefficients of F_1 are divisible by 11, our above computations for $k = 5$ and $p = 11$ show that there is a vector $\mathbf{y} = (y_1, \dots, y_6) \in (\mathbb{Z}_{11})^6$ such that $F_1(\mathbf{y}) = 0$. Also,

since F_2 contains 21 variables, there is a vector $\mathbf{z} = (z_7, \dots, z_{27})$ such that $F_2(\mathbf{z}) = 0$. For $1 \leq i \leq 6$ write $x_i = y_i Y_1$, and for $7 \leq i \leq 27$ write $x_i = z_i Y_2$. Then as in Section 2.2, the linear form becomes a form in two variables. This form has a nontrivial solution, which yields a nontrivial solution of the system. This completes the proof of Theorem 2.

REFERENCES

1. E. Artin, *Collected papers*, Addison-Wesley Pub. Co., Reading, Mass., 1965.
2. R. G. Bierstedt, *Some problems on the distribution of k th power residues modulo a prime*, Ph.D. thesis, University of Colorado, 1963.
3. R. Brauer, “A note on systems of homogeneous algebraic equations”, *Bull. Amer. Math. Soc.* **51** (1945), 749–755.
4. J. Brüdern and H. Godinho, “On Artin’s conjecture, II: pairs of additive forms”, *Proc. London Math. Soc.* **84** (2002), 513–538.
5. C. Chevalley, “Démonstration d’une hypothèse de M. Artin”, *Abh. Math. Sem. Hamburg* **11** (1935), 73–75.
6. S. Chowla, “On a conjecture of J. F. Gray”, *Norske Vid. Selsk. Forh. Trondheim* **33** (1960), 58–59.
7. H. Davenport and D. J. Lewis, “Homogeneous additive equations”, *Proc. Royal Soc. London Ser. A* **274** (1963), 443–460.

8. ———, “*Two additive equations*”, Proc. Symposia Pure Math. (Houston) **12** (1967), 74–98.
9. M. Dodson, “*Homogeneous additive congruences*”, Philos. Trans. Roy. Soc. London Ser. A **261** (1967), 163–210.
10. H. Godinho, J. F. Lima Neto, and P. H. A. Rodrigues, “*On pairs of additive congruences of odd degree*”, JP J. Algebra Number Theory Appl. **4** (2004), 55–78.
11. J. F. Gray, *Diagonal forms of prime degree*, Ph.D. thesis, University of Notre Dame, 1958.
12. M. Knapp, “*Diagonal equations of different degrees over p -adic fields*”, Acta Arith. **126.2** (2007), 139–154.
13. D. B. Leep and W. M. Schmidt, “*Systems of homogeneous equations*”, Invent. Math. **71** (1983), 539–549.
14. D. J. Lewis, “*Cubic homogeneous polynomials over p -adic number fields*”, Ann. of Math. (2) **56** (1952), 473–478.
15. K. K. Norton, *On homogeneous diagonal congruences of odd degree*, Ph.D. thesis, University of Illinois, 1966.
16. A. Tietäväinen, “*On a problem of Chowla and Shimura*”, J. Number Theory **3** (1971), 247–252.

Michael P. Knapp

Department of Mathematics and Statistics

Loyola University Maryland

4501 North Charles Street

Baltimore, MD 21210-2699

Email: mpknapp@loyola.edu