International Journal of Number Theory

Inhomogeneous Additive Equations

Michael P. Knapp

Department of Mathematics and Statistics
Loyola University Maryland
4501 North Charles Street
Baltimore, Maryland 21093, USA
mpknapp@loyola.edu

Received (Day Month Year)
Accepted (Day Month Year)

In this article, we study the function $\Delta^*(k,n)$, which we define as the smallest number s of variables needed to guarantee that the equation $\sum_{i=1}^{s} a_i x_i^k + \sum_{i=1}^{s} b_i y_i^n = 0$ has nontrivial solutions in each of the p-adic fields $\mathbb{Q}_p$, regardless of the rational integer coefficients. This generalizes the $\Gamma^*(k)$ function of Davenport & Lewis. In this article we give a sharp upper bound for $\Delta^*(k,n)$ and compute its value for various choices of the degrees.

Keywords: Additive polynomials; p-adic solubility.

Mathematics Subject Classification 2010: 11D72, 11D79 11D88

1. Introduction

Over the past 65 years, much study has been given to the problem of determining when an additive homogeneous polynomial is guaranteed to have p-adic integral zeros. Specifically, for a fixed prime p and degree k, one seeks to determine the smallest number s which guarantees that any polynomial of the form

$$a_1 x_1^k + a_2 x_2^k + \cdots + a_s x_s^k, \tag{1.1}$$

with integer coefficients, is guaranteed to have nontrivial p-adic integral zeros for every prime p. We define $\Gamma^*(k)$ to be this smallest such s. We then have

$$\Gamma^*(k) = \max_p \Gamma_p^*(k),$$

where $\Gamma_p^*(k)$ is the smallest s such that (**??**) has nontrivial zeros in $\mathbb{Z}_p^s$ for that specific prime p, where now the coefficients are allowed to be any p-adic (i.e., not only rational) integers. One of the earliest results in this area (see [**?**]) is that $\Gamma^*(k) \leq k^2 + 1$, with equality whenever $k+1$ is prime. Much work has been done to either find bounds on $\Gamma^*(k)$ when $k+1$ is composite (see for example [**?**,**?**,**?**,**?**]) or to find exact values of $\Gamma^*(k)$ for various degrees k (see [**?**,**?**,**?**,**?**,**?**,**?**,**?**,**?**], among others). More work has been done on the problem of solving systems of additive polynomials.

In this article, we study a multiple degree version of this problem. Given two (positive integer) degrees k and n, we seek the smallest number s which guarantees that the equation

$$\sum_{i=1}^{s} a_i x_i^k + \sum_{i=1}^{s} b_i y_i^n = 0$$

has nontrivial p-adic solutions for all primes p regardless of the rational integer coefficients. We will write this number as $\Delta^*(k,n)$. In analogy with the single degree problem, we define $\Delta_p^*(k,n)$ to be the smallest number of variables which guarantees p-adic solubility for the particular prime p. We then have

$$\Delta^*(k,n) = \max_p \Delta_p^*(k,n).$$

The function $\Delta^*(k,n)$ has some interesting properties. For instance, when $\gcd(k,n) = 1$, only one variable of each degree is required. We prove this in our first theorem.

Theorem 1.1. *Suppose that* $\gcd(k,n) = 1$*. Then* $\Delta^*(k,n) = 1$*.*

When considering upper bounds on $\Delta^*(k,n)$, we trivially have

$$\Delta^*(k,n) \leq \min\{\Gamma^*(k), \Gamma^*(n)\} \leq n^2 + 1.$$

In fact, we can do (very) slightly better than this, as we show in Theorem **??**.

Theorem 1.2. *For all k, n, we have $\Delta^*(k,n) \leq n^2$.*

Obviously, this immediately leads to the possibly better bound

$$\Delta^*(k,n) \leq \min\{k^2, n^2\}.$$

In light of Theorem **??**, it is perhaps surprising that Theorem **??** is in some sense best possible, as there are infinitely many pairs of degrees for which $\Delta^*(k,n) = n^2$. We prove this in Theorem **??**.

Theorem 1.3. *Let p be a prime, let $n = p - 1$, and let t be any integer such that $t \geq p(p-2)$. Then we have $\Delta_p^*(tn, n) = n^2$, and consequently $\Delta^*(tn, n) = n^2$.*

Noting that $\Gamma^*(n) = n^2 + 1$ when n is one less than a prime, it seems natural to make the following conjecture.

Conjecture 1.4. *Suppose that n is any positive integer. For all sufficiently large integers t, we have $\Delta^*(tn, n) = \Gamma^*(n) - 1$.*

The difficulty in proving this conjecture would likely be in dealing with degrees n such that $\Gamma^*(n) = \Gamma_p^*(n)$ for a prime p with $p|n$. When $p \nmid n$, a construction very similar to the one given in the proof of Theorem **??** should suffice to show that $\Delta_p^*(tn, n) = \Gamma_p^*(n) - 1$ for large enough values of t. This should work since in these cases, polynomials of degree n in $\Gamma_p^*(n) - 1$ variables with no nontrivial p-adic zeros can be constructed from polynomials in fewer variables which have no nontrivial zeros modulo p. This phenomenon no longer occurs when $p|n$, and so it is less clear what to do in that situation.

In our final two theorems, we calculate some more values of $\Delta^*(k, n)$. First, we calculate the value of $\Delta^*(k, 2)$ for all degrees k.

Theorem 1.5. *We have*

$$\Delta^*(k,2) = \begin{cases} 1 & \text{if } k \text{ is odd} \\ 3 & \text{if } k = 4 \\ 4 & \text{if } k \geq 6 \text{ and } k \text{ is even.} \end{cases}$$

In our last theorem, we calculate the value $\Delta^*(6, 4) = 7$. The proof (and also the proof that $\Delta^*(4, 2) = 3$ in Theorem **??**) shows some of the complexities that may arise in calculating values of $\Delta^*(k, n)$. We also note that the results of Theorem **??** and Theorem **??** may lead one to conjecture that $\Delta^*(k, n) \leq \Gamma^*(\gcd(k, n))$, and this example shows that such a conjecture would be false.

Theorem 1.6. *We have* $\Delta^*(6, 4) = 7$.

2. Preliminaries

In this section, we define the terms we will be using in our proofs and give some preliminary lemmas that we will need. We first show that it is enough to consider p-adic rational solutions of equations. In this lemma, and throughout the article, F will represent the polynomial

$$F = a_1 x_1^k + \cdots + a_s x_s^k + b_1 y_1^n + \cdots + b_s y_s^n, \tag{2.1}$$

where k, n are distinct positive integers and the a_i and b_i are p-adic integers.

Lemma 2.1. *Suppose that the equation* $F = 0$ *has a nontrivial solution in* $\mathbb{Q}_p^{2s}$. *Then it has a nontrivial solution in* $\mathbb{Z}_p^{2s}$. *Moreover, if there is a nontrivial solution in* $\mathbb{Z}_p^{2s}$, *then there is a solution in* $\mathbb{Z}_p^{2s}$ *in which either some* x*-variable is not divisible by* $p^{n/d}$ *or some* y*-variable is not divisible by* $p^{k/d}$, *where* $d = \gcd(k, n)$.

Proof. Note that for any $\mathbf{x}, \mathbf{y}$, we have

$$F(p^{n/d}\mathbf{x}, p^{k/d}\mathbf{y}) = p^{nk/d} F(\mathbf{x}, \mathbf{y}).$$

Hence, if $F(\mathbf{x}, \mathbf{y}) = 0$, then $F(p^{n/d}\mathbf{x}, p^{k/d}\mathbf{y}) = 0$. If $(\mathbf{x}, \mathbf{y}) \in \mathbb{Q}_p^{2s}$, then we can use this fact repeatedly to "clear" any powers of p from the denominators of the variables, ultimately arriving at a p-adic integral zero of F.

For the second statement, if $(\mathbf{x}, \mathbf{y}) \in \mathbb{Z}_p^{2s}$ is a nontrivial zero of F, then we have $F(p^{-n/d}\mathbf{x}, p^{-k/d}\mathbf{y}) = 0$. As above, using this transformation repeatedly will ultimately lead to non-integral zeros of F. In the last integral zero that we find by this method, either at least one of the x-variables is not divisible by $p^{n/d}$ or else at least one of the y-variables is not divisible by $p^{k/d}$. This completes the proof of the lemma. □

We next present a "normalization" lemma, which allows us to assume that the polynomial F has certain nice properties. This is essentially identical to [**?**, Lemma 2]. To state this lemma, we define the *level* of a variable as follows. If z is a variable in F whose coefficient is divisible by p^r, but not by p^{r+1}, then we say that z is *at level* r.

Lemma 2.2. *Suppose that p is a prime. In the polynomial F, we may assume without loss of generality that every variable is at a level which is less than its degree. Moreover, if we write $m_{k,i}$ for the number of variables of degree k at level i, and define $m_{n,i}$ similarly, then we may assume either that*

$$m_{k,0} + \cdots + m_{k,i-1} \geq \frac{is}{k} \quad \text{for} \quad 1 \leq i \leq k$$

or that

$$m_{n,0} + \cdots + m_{n,i-1} \geq \frac{is}{n} \quad \text{for} \quad 1 \leq i \leq n.$$

Proof. We only briefly sketch a proof of this. Suppose first that there is a variable x in F with coefficient a, and that $p^k | a$. Then we can make a change of variables of the form $x' = px$ to find a new form F' for which the power of p dividing the coefficient of x' is still positive, but smaller than the power of p dividing a.

By Lemma **??**, F' has a nontrivial p-adic integral zero if and only if F does. Using such transformations repeatedly proves the first assertion of the lemma. The second assertion follows immediately from [**?**, Lemma 2], after making a transformation of the general form

$$F' = \frac{1}{p^r} F(px_1, \ldots, px_i, x_{i+1}, \ldots, x_s, py_1, \ldots, py_j, y_{j+1}, \ldots, y_s), \qquad (2.2)$$

where r is as defined in [**?**, Lemma 2] and $x_1, \ldots, x_i, y_1, \ldots, y_j$ are the variables at levels less than r. □

Remark 2.3. Note that we may assume that either of the displayed equations in Lemma **??** holds, but we may not assume that they hold simultaneously. In particular, we may either assume that there are at least s/k of the x-variables at level 0, or that there are at least s/n of the y-variables at level 0, but we may not assume that level 0 contains both s/k x-variables and s/n y-variables. It is possible (although we will not do so here) to develop a normalization theory which gives information about the total number of variables at different levels. For instance, we can show that we may assume that there are at least $(n+k)s/nk$ variables in total at level 0, but with this normalization we cannot make any assumptions about how many of these are x-variables and how many are y-variables.

We will find p-adic zeros of F through the use of Hensel's lemma. Therefore we give a version of this lemma here.

Lemma 2.4. *Suppose that p is a fixed prime and write $k = p^{\tau_k} k_0$, where k_0 is not divisible by p. Define the number γ_k by*

$$\gamma_k = \begin{cases} \tau_k + 2 & \text{if } p = 2 \text{ and } \tau_k \geq 1 \\ \tau_k + 1 & \text{otherwise.} \end{cases}$$

Let h be a positive integer. Suppose that we can solve the congruence $F \equiv 0 \pmod{p^{h+\tau_k}}$ in such a way that a variable of degree k at level at most h is not divisible by p. Then the solution of this congruence can be lifted to a p-adic integral solution of $F = 0$.

Of course, we can replace k by n in Lemma **??** if we wish. We will typically use this lemma in the following fashion. Suppose that the part of F at some level ℓ is given by

$$p^{\ell}(a_1x_1^k + \cdots + a_ux_u^k + b_1y_1^n + \cdots + b_vy_v^n).$$

If we can solve the congruence

$$a_1x_1^k + \cdots + a_ux_u^k + b_1y_1^n + \cdots + b_vy_v^n \equiv 0 \pmod{p^{\tau_k}} \tag{2.3}$$

with some variable x_i not divisible by p, then we can find a nontrivial p-adic zero of F. In this case, we say that the solution of (**??**) is *nonsingular at* x_i.

Our next four lemmas will be used to help us solve congruences. The first is the well-known Cauchy-Davenport theorem and the next two have the same flavor. The fourth is a very useful lemma due to Bovey allowing us to find zeros of polynomials modulo a power of 2.

Lemma 2.5 (Cauchy-Davenport [?]). *Let A, B be sets of residues modulo a prime p. Write $|S|$ for the number of elements in the set S, and define*

$$A + B = \{a + b \,:\, a \in A \text{ and } b \in B\}.$$

Then we have

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

Lemma 2.6 (Chowla-Mann-Straus [?, Theorem 3]). *Let*

$$a_1a_2\cdots a_t \not\equiv 0 \pmod{p} \quad \text{and} \quad \gcd(p-1, k) < \frac{p-1}{2}.$$

Then the expression $a_1x_1^k + \cdots + a_tx_t^k$ either represents all residues modulo p or else represents at least $(2t-1)\frac{p-1}{\gcd(p-1,k)} + 1$ residues modulo p.

Lemma 2.7 (Davenport-Lewis [?, Lemma 1]). *Let p be a prime, let k divide $p-1$, and let $a_1a_2\cdots a_t \not\equiv 0 \pmod{p}$. Then if $t \leq k$, the number of distinct residue classes modulo p other than 0 represented by the expression $a_1x_1^k + \cdots + a_tx_t^k$ is at least $t(p-1)/k$.*

Lemma 2.8 (Bovey [?, Lemma 1]). *Let ℓ be a positive integer and suppose that for $i = 0, \ldots, \ell$, we have $F_i = \sum_{j=1}^{v_i} a_{ij} x_{ij}$ with all the a_{ij} odd and with $\sum_{i=0}^{h-1} v_i \geq 2^h$ for each $h = 1, \ldots, \ell$. Then for any positive integer $L > \ell$, the expression $\sum_{i=0}^{\ell} 2^i F_i$ represents at least $\min\left(\sum_{i=0}^{\ell} v_i, 2^L\right)$ different residues modulo 2^L where the $x_{ij} = 0$ or 1 and with at least one of the $x_{0j} = 1$.*

While the above lemma is written specifically in terms of linear polynomials, it is easily applied in our situation, as $x^k = x^n = x$ when $x \in \{0, 1\}$.

Our final lemma will allow us to make certain desirable changes of variables during our proofs.

Lemma 2.9. *Let $d = \gcd(k, n)$ and suppose that $\ell_x \equiv \ell_y \pmod{d}$. Then we can make a change of variables to create a polynomial F' such the x-variables at level ℓ_x of F and the y-variables at level ℓ_y of F end up at the same level in F'.*

Proof. Suppose without loss of generality that $\ell_x > \ell_y$. We can write $\ell_x = \ell_y + dt$ for some positive integer t. Moreover, we can write $k = dk'$ and $n = dn'$, where $\gcd(k', n') = 1$. We make our change of variables as follows. For every x-variable at level ℓ_x in F, we set $x = p^u x'$ and for every y-variable at level ℓ_y of F, we set $y = p^v y'$. Then in F' the variables x' appear at level $\ell_x + ku$ and the variables y' appear at level $\ell_y + nv$. Our goal is then to choose u and v such that $\ell_x + ku = \ell_y + nv$. We can do this if and only if we can solve $t + k'u = n'v$. But this final equation must have positive integer solutions since k' and n' are relatively prime. This completes the proof of the lemma. □

3. The Value of $\Delta^*(k, n)$ when $\gcd(k, n) = 1$

In this section, we give the short proof of Theorem **??**, that $\Delta^*(k, n) = 1$ when $\gcd(k, n) = 1$. Suppose that p is a prime. We need to show that any equation

$$ax^k + by^n = 0$$

has a solution in $\mathbb{Z}_p$. Since $\gcd(k, n) = 1$, Lemma **??** shows that we can make a change of variables to obtain an equivalent equation

$$p^\ell(a'x^k + b'y^n) = 0$$

where neither a' nor b' is divisible by p. By Lemma **??** and the subsequent discussion, it suffices to find a nontrivial solution of

$$a'x^k + b'y^n \equiv 0 \pmod{p}. \tag{3.1}$$

Since $\gcd(k, n) = 1$, at least one of k, n is not divisible by p, and hence any nontrivial solution of (**??**) will be nonsingular in at least one of the variables. Multiplying the entire congruence by $(a')^{-1} \pmod{p}$, we may assume that $a' = 1$.

Suppose first that $p \neq 2$. Let g be a primitive root modulo p, and note that we have $-1 \equiv g^{(p-1)/2} \pmod{p}$. Suppose that $b' \equiv g^r \pmod{p}$, and write $x = g^u$ and $y = g^v$. Then we can find a nontrivial solution of (**??**) if and only if we can find integers u, v with $ku - nv \equiv r + (p-1)/2 \pmod{p-1}$. However, since $\gcd(k, n) = 1$, we can even find u, v with $ku - nv = r + (p - 1)/2$. This completes the proof for these primes.

If $p = 2$, then (**??**) is the congruence $x^k + y^n \equiv 0 \pmod{2}$, and one solution of this is $x = y = 1$. Since at least one of the degrees must be odd, this solution is nonsingular in at least one variable. Thus the proof is complete in this case as well.

□

Remark 3.1. We prove Theorem **??** via Hensel's Lemma in order to deal with values of the coefficients that are not rational integers. If we assume that $a, b \in \mathbb{Z}$, then we could give an even shorter proof by considering the prime factorizations of a, b, x^k, and y^n.

4. Upper Bounds for $\Delta^*(k, n)$

In this section, we prove Theorem **??**, that we always have $\Delta^*(k, n) \le n^2$. If $n = 1$, then we are done by Theorem **??**, so we assume that $n \ge 2$. We begin by quickly showing that $\Delta_p^*(k, n) \le n^2$ except possibly in the case where $n = p - 1$ and the case where $n = 2$ (with p arbitrary). This follows from a number of results already present in the literature.

If $n \ge 13$ is odd, then [**?**, Theorem 3] shows that $\Gamma^*(n) \le (n^2 + 1)/2$. For other odd values of n, we know that $\Gamma^*(n) < n^2$ by results of Bierstedt [**?**] (for $n = 7, 11$), Norton [**?**] ($n = 5, 7, 9, 11$), Dodson [**?**] ($n = 9, 11$), and Lewis [**?**] ($n = 3$). The combined work of Gray [**?**] and Chowla [**?**] also gives the result for $n = 5$. In light of the bound $\Delta^*(k, n) \le \Gamma^*(n)$, these results give us Theorem **??** for all odd n.

Suppose next that n is even and $n \ge 4$. If p is an odd prime such that $n \ne p - 1$ and $n \ne p(p - 1)$, then work of Brüdern & Robert (see the proofs of [**?**, Lemmas 3.4 and 3.5]) shows that $\Gamma_p^*(n) \le \frac{1}{2}n^2 + 1$. Moreover, if p is odd and $n = p(p - 1)$, then Godinho, et al. show [**?**, Theorem 1] that $\Gamma_p^*(n) = \frac{1}{2}n^2\left(1 + \frac{1}{p}\right) + 1$, which is less than n^2. Finally, if $p = 2$, then the main theorem of [**?**] gives an exact formula for $\Gamma_2^*(n)$ which can be seen to be at most n^2 whenever $n \ge 4$. Again, in light of the bound $\Delta^*(k, n) \le \Gamma^*(n)$, we see that Theorem **??** is true for these choices of n and p.

We now treat the remaining cases. Suppose first that $n = p - 1$, where p is an odd prime, and let $s = n^2$. As indicated in Lemma **??**, we may assume that each variable of degree n is at level at most $n - 1$. If any level ℓ contains at least $n + 1$ variables of degree n, then Chevalley's theorem allows us to find a nontrivial solution of the congruence $F \equiv 0 \pmod{p^{\ell+1}}$ using only the variables of degree n at level ℓ, and we are done by Lemma **??**. Otherwise, each of levels $0, 1, \ldots, n - 1$

contains exactly n variables of degree n. Suppose that x is any variable of degree k. Then we can make a change of variables of the general type (**??**) so that there are n variables of degree n at the same level ℓ as x. If there are any variables of degree k at level ℓ other than x, we set them equal to zero. Then the portion of F at this level looks like

$$p^\ell \left(ax^k + b_1y_1^n + \cdots + b_ny_n^n\right).$$

By Lemma **??**, the expression $b_1y_1^n + \cdots + b_ny_n^n$ represents every nonzero residue modulo p. Set $x = 1$ and choose $y_1, \ldots, y_n$ so that $b_1y_1^n + \cdots + b_ny_n^n \equiv -a \pmod{p}$. We now have a nonsingular solution of $F \equiv 0 \pmod{p^{\ell+1}}$, which lifts to a p-adic zero of F as noted above.

We now turn to the case when $n = 2$. If k is odd then we are done by Theorem **??**. Suppose that k is even and $s = 4$. We first treat the case when p is odd. As before, by Lemma **??** we can assume that all the variables of degree 2 are at level either 0 or 1, and that at least two of these variables are at level 0. By either Lemma **??** or Lemma **??**, any expression $a_1y_1^2 + a_2y_2^2$ with $p \nmid a_1a_2$ represents every nonzero residue modulo p. If there is any additional variable (of either degree) at level 0, then we may set this variable equal to 1 and then use the two y-variables to complete this to a solution of $F \equiv 0 \pmod{p}$, which lifts to a p-adic zero of F.

Otherwise, there are two y-variables at level 0 and two more at level 1. Suppose that there is an x-variable at level r. Choose $r^* \in \{0, 1\}$ so that $r^* \equiv r \pmod{2}$. By Lemma **??**, we may make a change of variables of the form (**??**) to produce a new polynomial F' such that the x-variable at level r and the y-variables at level r^* of F end up at the same level ℓ in F'. Then with these three variables we can nontrivially solve the congruence $F' \equiv 0 \pmod{p^{\ell+1}}$ as above, and this solution lifts to a p-adic zero of F. This completes the proof in the case when $n = 2$ and p is odd.

Finally, we treat the case in which $p = n = 2$. Again, we may assume that every variable in F is at a level less than its degree. If we can find a solution of the congruence $F \equiv 0 \pmod 8$ which uses only the degree 2 variables and in which there is at least one variable at level 0 with an odd value, then this solution lifts to a 2-adic solution by Lemma **??**. One can check that if there is no such solution, then the degree 2 part of F, considered modulo 8, must look like one of the following five possibilities (perhaps multiplied by an odd number or with the variables renamed):

$$\begin{aligned}
&y_1^2 + y_2^2 + y_3^2 + y_4^2 \\
&y_1^2 + y_2^2 + 2y_3^2 + 2y_4^2 \\
&y_1^2 + y_2^2 + 5y_3^2 + 5y_4^2 \\
&y_1^2 + 3y_2^2 + 2y_3^2 + 6y_4^2 \\
&y_1^2 + 5y_2^2 + 6y_3^2 + 6y_4^2.
\end{aligned}$$

Note that each of these polynomials represents every nonzero residue modulo 8 with at least one variable at level 0 equal to 1. Now, if necessary, make successive changes of variables of the form

$$F' = \frac{1}{p^2} F(x_1, x_2, x_3, x_4, 2y_1, 2y_2, 2y_3, 2y_4) \tag{4.1}$$

until the resulting polynomial has a variable x_i of degree k at level either 0 or 1, and note that the degree 2 part of F' is identical to the degree 2 part of F. Then as above, we can solve the congruence $F' \equiv 0 \pmod 8$ with $x_i = 1$ and at least one of the y-variables at level 0 equal to 1. This solution lifts to a 2-adic zero of F'. Since F' has a nontrivial 2-adic zero, so does F, completing the proof of Theorem **??**. □

5. Large Values of $\Delta^*(k, n)$

Now that we have shown that $\Delta^*(k, n) \le n^2$, we show that this upper bound can actually be obtained by proving Theorem **??**. To prove this theorem, it suffices to give an example of a polynomial with $n^2 - 1$ variables of each degree which has no nontrivial p-adic zeros. Our example is the following. As in the statement of the theorem, let p be a prime, let $n = p - 1$, and let $k = tn$ with $t \geq p(p-2)$. Let $\mathbf{z} = (z_1, \ldots, z_{n-1})$ be an $(n-1)$-tuple of variables and let $\mathbf{y}_i = (y_{i,1}, \ldots, y_{i,n})$ be an n-tuple of variables. Define

$$G_z(\mathbf{z}) = z_1^n + z_2^n + \cdots + z_{n-1}^n$$

and

$$G_y(\mathbf{y}_i) = y_{i,1}^n + y_{i,2}^n + \cdots + y_{i,n}^n.$$

Thus the only difference between G_z and G_y is that G_y contains one extra variable. Then our polynomial is

$$F = G_z(\mathbf{z}) + \sum_{i=1}^{n-1} p^i G_y(\mathbf{y}_i) + \sum_{i=1}^{n^2-1} p^{(i-1)n} x_i^k.$$

That is, we set

$$F = G_z(\mathbf{z}) + pG_y(\mathbf{y}_1) + p^2 G_y(\mathbf{y}_2) + \cdots + p^{n-1} G_y(\mathbf{y}_{n-1}) \\ + x_1^k + p^n x_2^k + p^{2n} x_3^k + \cdots + p^{n^3-2n} x_{n^2-1}^k.$$

By Lemma **??**, if the equation $F = 0$ has any nontrivial p-adic integral solutions, then it has one with either some x_i not divisible by p or some z_i or $y_{i,j}$ not divisible by p^t. We will show that the congruence $F \equiv 0 \pmod{p^k}$ has no solutions satisfying these conditions.

In order to solve the congruence $F \equiv 0 \pmod{p^k}$, we first need to solve

$$z_1^n + \cdots + z_{n-1}^n + x_1^k \equiv 0 \pmod{p}.$$

Since the only n-th and k-th powers modulo p are 0 and 1, the only solution of this congruence is to have each of these variables divisible by p. Making the substitution $z_i = pz_i'$, $x_1 = px_1'$, we see that the z-variables are moved to level n and x_1 is moved to level k. Thus x_1 will no longer play a role in solving $F \equiv 0 \pmod{p^k}$. Using similar logic to solve $F \equiv 0$ modulo $p^2, p^3, \ldots, p^n$, we see that each variable $y_{i,j}$

must be divisible by p. Hence we may make the change of variables $y_{i,j} = py'_{i,j}$.

These changes of variables result in the polynomial

$$F' = p^n G_z(\mathbf{z}') + \sum_{i=1}^{n-1} p^{n+i} G_y(\mathbf{y}'_i) + \sum_{i=2}^{n^2-1} p^{(i-1)n} x_i^k + p^k (x'_1)^k.$$

We can now reason exactly as above (looking modulo $p^{n+1}, p^{n+2}, \ldots, p^{2n}$) to see that each of the variables z'_i, $y'_{i,j}$, and x_2 must be divisible by p. That is, each of the variables z_i and $y_{i,j}$ must be divisible by p^2, while x_1 and x_2 must both be divisible by p. Repeating this argument until we eventually study the congruence $F \equiv 0 \pmod{p^k}$, we see that each of the variables z_i and $y_{i,j}$ must be divisible by p^t and each of the variables x_i must be divisible by p. This provides a contradiction, showing that the only p-adic solution of $F = 0$ is the trivial solution.

This gives us $\Delta_p^*(k,n) > n^2 - 1$ for this choice of p, n, k. Combined with Theorem **??**, we see that $\Delta_p^*(k,n) = n^2$, and hence $\Delta^*(k,n) = n^2$. □

Remark 5.1. This is indeed a maximal example, as adding one more variable of each degree (or even just one more variable of degree n) will produce a polynomial which does have nontrivial p-adic zeros. However, we note that we could add more terms of the form x_i^k, one at each level less than k which is a multiple of $p-1$, and still have a polynomial with only the trivial zero.

Remark 5.2. It would also be interesting to eliminate the condition that each degree have an equal number of variables and study the function which returns the least total number of variables that guarantees that $F = 0$ has nontrivial solutions. This function would have properties different from those of $\Delta^*(k,n)$. For example, its value would always be at least $\max\{\Gamma^*(k), \Gamma^*(n)\}$ due to the possibility that all the variables in F have the same degree.

6. The Value of $\Delta^*(k, 2)$

In this section we give the proof of Theorem **??**. If k is odd, then the result follows immediately from Theorem **??**. Moreover, if $k = 2k_0$ with $k_0 \geq 3$, then Theorem **??** gives $\Delta^*(k, 2) = 4$. Hence we need only to show that $\Delta^*(4, 2) = 3$.

We begin the proof by showing that $\Delta_p^*(4, 2) = 3$ whenever p is odd. To see this, we first find an example of a polynomial with $s = 2$ and no nontrivial p-adic zeros. Let Q be any integer such that $-Q$ is not a square modulo p. Then the congruence $y_1^2 + Qy_2^2 \equiv 0 \pmod{p}$ has no nontrivial solutions, and one can show that the polynomial

$$px_1^4 + p^3x_2^4 + y_1^2 + Qy_2^2$$

has no nontrivial p-adic zeros. We omit the proof of this, which is similar to the one given in the previous section.

Now let $s = 3$. As before, Lemma **??** allows us to assume that each variable is at a level smaller than its degree, and that at least two variables of degree 2 are at level 0. If all three quadratic variables are at level 0, then we are done by Chevalley's theorem and Lemma **??**. Otherwise, after perhaps multiplying F by a constant, the y-variables in F look like

$$y_1^2 + b_2y_2^2 + pb_3y_3^2,$$

where $p \nmid b_2b_3$. We may also assume that the congruence $y_1^2 + b_2y_2^2 \equiv 0 \pmod{p}$ has no nontrivial solutions, as any nontrivial solution would lift to a p-adic solution. Now, the expression $y_1^2 + b_2y_2^2$ will represent all nonzero residues modulo p by either Lemma **??** or Lemma **??**. Hence if there is a variable x of degree 4 at level 0, we may set $x = 1$ and extend this to a nonsingular solution of the congruence $F \equiv 0 \pmod{p}$. Similarly, if there is a variable of degree 4 at level 2, then we can make a change of variables which moves y_1 and y_2 to level 2, after which the same argument applies. Therefore we may assume that all of the x-variables are at levels 1 and 3.

In this case, either level 1 or level 3 contains at least two x-variables. If necessary, we use Lemma **??** to make a change of variables which produces a polynomial F' such that these two x-variables and the y-variable at level 1 of F end up at the same level ℓ in F'. That is, the part of F' at level ℓ looks like

$$p^\ell \left(a_1 x_1^4 + a_2 x_2^4 + b_3 y_3^2\right),$$

where $p \nmid a_1 a_2 b_3$. (If F' has an additional variable at level ℓ, we set it equal to 0.) If $p \equiv 3 \pmod 4$, then we have $\gcd(4, p-1) = 2$, and the set of 4th powers modulo p is the same as the set of squares modulo p. Therefore as before we can solve the congruence

$$a_1 x_1^4 + a_2 x_2^4 + b_3 y_3^2 \equiv 0 \pmod p \tag{6.1}$$

nontrivially by Chevalley's theorem, and this solution lifts to a p-adic solution. If $p \equiv 1 \pmod 4$ and $p > 5$, then a result [**?**, Theorem 7] of Chowla, Mann, & Straus shows that the expression $a_2 x_2^4 + b_3 y_3^2$ represents every nonzero residue modulo p. Hence we may set $x_1 = 1$ and complete this to a nontrivial (and hence nonsingular) solution of (**??**) as above.

Finally, suppose that $p = 5$ and consider the congruence (**??**). Again, any nontrivial solution of this congruence will lead to a 5-adic zero of F. Dividing (**??**) through by b_3, we may assume that $b_3 = 1$. If either of a_1, a_2 is congruent to 1 or $4 \pmod 5$, then we can get a nontrivial solution using that variable and y_3. Moreover, if $a_1 + a_2 \equiv 0 \pmod 5$, then setting $(x_1, x_2, y_3) = (1, 1, 0)$ gives a nontrivial solution of (**??**). The only remaining possibilities are $a_1 = a_2 = 2$ and $a_1 = a_2 = 3$. In the first case, $(x_1, x_2, y_3) = (1, 1, 1)$ is a nontrivial solution of (**??**), and in the second case $(x_1, x_2, y_3) = (1, 1, 2)$ works. This completes the proof that $\Delta_p^*(4, 2) = 3$

whenever p is odd.

It remains to consider $\Delta_2^*(4,2)$. Suppose that $s = 3$. As before, we may assume that all the y-variables are at levels 0 and 1, and that all of the x-variables are at levels 0, 1, 2, and 3. If necessary, we may make a change of variables of the form (**??**) so that in addition to the y-variables, levels 0 and 1 together contain at least two x-variables. Set the remaining x-variable equal to 0. Then we have

$$F = a_1x_1^4 + a_2x_2^4 + b_1y_1^2 + b_2y_2^2 + b_3y_3^2,$$

where b_1 and b_2 are odd and none of the coefficients are divisible by 4. We show that we can solve

$$F \equiv 0 \pmod 8 \tag{6.2}$$

with at least one of y_1, y_2 not divisible by 2. By multiplying (**??**) by a unit, we may assume that $b_1 = 1$, and hence that $b_2, b_3 \neq 7$. We may also assume that if b_3 is at level 0, then $b_2 \leq b_3$. With these assumptions, there are 12 possibilities for the 3-tuple (b_1, b_2, b_3). If we eliminate the ones such that (**??**) has a nonsingular solution involving only the y-variables, then this 3-tuple must be one of

$$\begin{array}{ll} (1,1,1) & (1,3,6) \\ (1,1,2) & (1,5,5) \\ (1,1,5) & (1,5,6). \\ (1,3,2) & \end{array}$$

Suppose that $(b_1, b_2, b_3) = (1, 5, 6)$. Then using only the y-variables, we can represent every nonzero residue modulo 8 nonsingularly (i.e., with at least one odd variable at level 0) except for 2 and 4. Since $a_1 \neq 4$, we can solve (**??**) nonsingularly using only x_1 and the y-variables unless $a_1 = 6$. Similarly, we can find a nonsingular solution of (**??**) whenever $a_2 \neq 6$. Thus in this case we can solve (**??**) nonsingularly except possibly for the congruence

$$6x_1^4 + 6x_2^4 + y_1^2 + 5y_2^2 + 6y_3^2 \equiv 0 \pmod 8.$$

However, we can see that $(\mathbf{x}, \mathbf{y}) = (1, 1, 1, 1, 1)$ is a nonsingular solution of this final congruence. The other possible values for (b_1, b_2, b_3) can be treated similarly, and we omit the details. This shows that $\Delta_2^*(4, 2) \le 3$, completing the proof of Theorem **??**.

□

7. The Value of $\Delta^*(6, 4)$

Finally, we prove Theorem **??**, that $\Delta^*(6, 4) = 7$. First, consider the form

$$F = (x_1^6 + 2x_2^6) + 5(y_1^4 + y_2^4 + y_3^4) + 5^2(x_3^6 + 2x_4^6) + 5^3(y_4^4 + y_5^4 + y_6^4) + 5^4(x_5^6 + 2x_6^6).$$

In the same manner as we have before, we can show that F has no nontrivial 5-adic zeros. This shows that $\Delta^*(6, 4) \ge 7$. Now we need to show that having seven variables of each degree guarantees p-adic solutions for all p.

Suppose that $s = 7$ and that every variable is at a level less than its degree. Note that the x-variables now have degree 6 and the y-variables have degree 4. For now, suppose that $p \ge 7$. Then Lemma **??** shows that the expression $b_1 y_1^4 + b_2 y_2^4 + b_3 y_3^4$ (with $p \nmid b_1 b_2 b_3$) represents every nonzero residue modulo p. Therefore, if there is a level with at least four y-variables, then we may set one of those variables equal to 1 and use the other three to complete a nonsingular solution of an appropriate congruence, and we are done. Hence, for these primes we may assume that every level contains at most three y-variables.

Now suppose that some level ℓ does contain three y-variables. If there is any x-variable at level ℓ, then we can set it equal to 1 and proceed as above to find a p-adic zero of F. Otherwise, every x-variable is at a level different from ℓ. In fact the x-variables must all be at levels of different parity from ℓ, as otherwise we could use Lemma **??** to create a level with an x-variable and three y-variables. Thus the x-variables are distributed among only three levels, and so there must be a level ℓ' containing at least three of them. Moreover, since each level has at most three

y-variables, there must be a y-variable at a level of the same parity as ℓ'. Using Lemma **??** again, we may create a level with three x-variables and a y-variable. If $\gcd(p-1,6) < \frac{p-1}{2}$, then by Lemma **??** the three x-variables represent at least $\frac{5}{6}(p-1)+1$ residues modulo p, and Lemma **??** shows that if we set the y-variable to a nonzero value, then we represent at least

$$\min\left\{p, \left(\frac{5}{6}(p-1)+1\right) + \frac{p-1}{4} - 1\right\} = \min\left\{p, \frac{13}{12}(p-1)\right\} > p-1$$

residues modulo p. Since the number of residues represented must be an integer, we see that zero is represented nontrivially, and hence nonsingularly. So we are done in this case as well (provided that $\gcd(p-1,6) < (p-1)/2$).

Finally, we treat the case in which each level has at most two y-variables. In this situation, there must be levels of both parities which contain two y-variables. Since some level must contain two x-variables, we can make a change of variables to create a level with two variables of each degree. By Lemma **??**, the two y-variables represent at least $\frac{3}{4}(p-1)+1$ residues modulo p. Lemma **??** shows that adding one x-variable allows us to represent at least $\frac{11}{12}(p-1)+1$ residues modulo p. Finally, if we set the last x-variable to a nonzero value, then Lemma **??** shows that we may represent at least

$$\min\left\{p, \frac{13}{12}(p-1)\right\} > p-1$$

residues modulo p. As above, we see that we can nontrivially (and hence nonsingularly) represent 0, and we are done.

The above work suffices to show that $\Delta_p^*(6,4) \leq 7$ for all primes except $p = 2, 3, 5, 7, 13$. We deal with these primes individually. Suppose first that $p = 13$. The above proof works for this prime except for the situation in which there is a level with three x-variables and one y-variable, so assume that this occurs. At this level, we need to solve a congruence of the form

$$a_1x_1^6 + a_2x_2^6 + a_3x_3^6 + by^4 \equiv 0 \pmod{13}, \tag{7.1}$$

where $13 \nmid a_1a_2a_3b$. Define

$$R = \{a_1x_1^6 + a_2x_2^6 + a_3x_3^6 \pmod{13}\}$$

and

$$R' = \{a_1x_1^6 + a_2x_2^6 + a_3x_3^6 \pmod{13} \,:\, x_i \in \{0,1\}\}.$$

If $|R'| < 8$, then there is a residue in R' which can be obtained in two different ways, and this leads to a nontrivial solution of (**??**) by a well-known argument (see for example the proof of [**?**, Lemma 2.2.1]). So we may assume that $|R'| = 8$, and therefore that $|R| \geq 8$. Note that R has the property that if $a \in R$ then $-a \in R$. Since the possible nonzero values of by^4 are b, $3b$, and $9b$, if any of the residues

$$b, -b, 3b, -3b, 9b, -9b$$

are in R, then we can find a nontrivial solution of our congruence. But these residues are distinct modulo 13, and hence at least one of them must be contained in R since $|R| \geq 8$. This completes the proof in this case, and therefore completes the proof that $\Delta_{13}^*(6,4) \leq 7$.

Suppose now that $p = 7$ or $p = 3$. The same argument works for both of these primes. As we have seen, if we have two y-variables at the same level, then these terms represent every nonzero residue modulo p. Therefore, if some level contains two y-variables and any additional variable, then one can find a nonsingular solution of a congruence as before, and hence a p-adic zero of F. But as we have seen, there must either be a level with three y-variables or (perhaps after a change of variables of the form (**??**)) a level with two y-variables and two x-variables. Hence there are p-adic zeros of F, and so $\Delta_p^*(6,4) \leq 7$ for these two primes.

If $p = 5$, then a similar argument works. By Lemma **??**, any expression of the form $a_1x_1^6 + a_2x_2^6$ must represent all nonzero residues modulo 5. Hence if any level contains two x-variables and any other variable, then one can find a nonsingular solution of a congruence, and hence a 5-adic zero of F. Suppose that this does not happen, even after any possible change of variables. Since at least one level ℓ must contain two x-variables, the y-variables must be distributed among the two allowable levels with parity different from ℓ. However, this means that there must be a level ℓ' which has four y-variables, which represent all nonzero residues modulo 5 by Lemma **??**. Since no level contains three x-variables, there must be an x-variable at a level of the same parity as ℓ'. Then we may make a change of variables so that some level contains four y-variables and an x-variable. With these variables, we can find a nonsingular solution of an appropriate congruence, and hence a 5-adic zero of F. Therefore $\Delta_5^*(6, 4) \leq 7$.

Finally, we deal with the case $p = 2$. This is the most difficult case. As always, we assume that each variable is at a level lower than its degree. As in Section **??** write $m_{6,i}$ for the number of x-variables (of degree 6) at level i in F. By Lemma **??**, we may assume that

$$
\begin{aligned}
m_{6,0} &\geq 2 \\
m_{6,0} + m_{6,1} &\geq 3 \\
m_{6,0} + m_{6,1} + m_{6,2} &\geq 4.
\end{aligned}
$$

Suppose first that $m_{6,1} \geq 1$ and $m_{6,2} \geq 1$. Set two x-variables at level 0 equal to 1. This gives a solution of $F \equiv 0 \pmod{2}$. If it is not a solution of $F \equiv 0 \pmod{4}$, then set one of the variables at level 1 equal to 1. This gives a solution of $F \equiv 0 \pmod{4}$. If it is not a solution of $F \equiv 0 \pmod{8}$, then we can solve this final congruence by setting one of the variables at level 2 equal to 1. Then we have found a nonsingular solution of $F \equiv 0 \pmod{8}$, which lifts to a 2-adic zero of F.

We now need to treat the cases where $m_{6,1} = 0$ or $m_{6,2} = 0$. We begin with the case in which $m_{6,2} = 0$. By Lemma **??**, we have $m_{6,0} \geq 2$ and $m_{6,0} + m_{6,1} \geq 4$. If there are y-variables at level 2, then Lemma **??** shows that we can use the x-variables at levels 0 and 1 to solve the congruence $F \equiv 0 \pmod{4}$ with at least one odd variable at level 0. If necessary, we can then use the variable at level 2 to complete this to a solution modulo 8, in which case we are done. If there are y-variables at level 0, then the same argument works after the change of variables $F' = \frac{1}{2^6} F(2\mathbf{x}, 4\mathbf{y})$. Hence we may assume that all of the y-variables are at levels 1 and 3. One of these levels must contain at least four y-variables. If these four y-variables are at level 1, then we have two x-variables at level 0 and at least eight total variables at levels 0 and 1. By Lemma **??**, we can use these variables to find a nonsingular solution of the congruence $F \equiv 0 \pmod{8}$. If the four y-variables are at level 3, then we can make the change of variables $F' = F(2\mathbf{x}, 2\mathbf{y})$. If there are any y-variables at level 5 of F', we set them to 0 and then divide F' by 2^6. The resulting polynomial has two x-variables at level 0 and at least eight total variables at levels 0 and 1, so we may finish the proof as above. This completes the proof in the case when $m_2 = 0$.

Suppose instead that $m_{6,2} \geq 1$ and $m_{6,1} = 0$. Then Lemma **??** guarantees that $m_{6,0} \geq 3$. If there is a y-variable at level 0, then Lemma **??** shows that we may use the variables at level 0 to solve the congruence $F \equiv 0 \pmod{4}$. Note that in this solution there must be at least one odd x-variable. If we actually have a solution modulo 8, then we are done. Otherwise, we may extend this to a solution modulo 8 using a variable at level 2, and we are done. On the other hand, suppose that there are no y-variables at level 0. If there is a y-variable at level 2, then after the change of variables $F' = F(2\mathbf{x}, 2\mathbf{y})$, the same argument works (after perhaps setting some variables to 0 and dividing F' by 2^6). Hence we may assume that all the y-variables are at levels 1 and 3. One of these levels must contain at least four y-variables. If these variables are at level 1, then we can use the x-variables at level 0 and the y-variables at level 1 to solve the congruence $F \equiv 0 \pmod 4$ with the x-variables odd. If necessary, we can then use an x-variable at level 2 to extend this to a nonsingular solution modulo 8. If the four y-variables are at level 3, then the same argument works after the change of variables $F' = F(2\mathbf{x}, 2\mathbf{y})$ and possibly setting some variables equal to 0 and dividing F' by 2^6. This finishes the proof in this case, and completes the proof of Theorem **??**.

□

References

[1] R. G. Bierstedt, Some problems on the distribution of kth power residues modulo a prime, Ph.D. Thesis, University of Colorado, 1963.

[2] J. D. Bovey, $\Gamma^*(8)$, *Acta Arith.* **25** (1974) 145-150.

[3] C. Broll, J. Jennings, M. Knapp, P. H. A. Rodrigues and D. Veras, More exact values of the function $\Gamma^*(k)$, (in preparation).

[4] J. Brüdern and O. Robert, On Artin's conjecture: linear slices of diagonal hypersurfaces, *Trans. Amer. Math. Soc.* **372** (2019) 1867-1911.

[5] S. Chowla, On a conjecture of J. F. Gray, *Norske Vid. Selsk. Forh. Trondheim* **33** (1960) 58-59.

[6] S. Chowla, H. B. Mann and E. G. Straus, Some applications of the Cauchy-Davenport theorem, *Norske Vid. Selsk. Forh. Trondheim* **32** (1959) 74-80.

[7] H. Davenport, On the addition of residue classes, *J. London Math. Soc.* **10** (1935) 30-32.

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

[9] H. Davenport and D. J. Lewis, Notes on congruences (III), *Quart. J. Math. Oxford Ser. (2)* **17** (1966) 339-344.

[10] M. Dodson, Homogeneous additive congruences, *Philos. Trans. Roy. Soc. London Ser. A* **261** (1967) 163-210.

[11] H. Godinho and M. Knapp, Infinitely many counterexamples to a conjecture of Norton, *Michigan Math. J.* advance publication, 22 January 2020. doi:10.1307/mmj/1579683616.

[12] H. Godinho, M. Knapp, P. H. A. Rodrigues and D. Veras, On the values of $\Gamma^*(k,p)$

and $\Gamma^*(k)$, *Acta Arith.* **191**(1) (2019) 67-80.

[13] J. F. Gray, Diagonal forms of prime degree, Ph.D. Thesis, University of Notre Dame, 1958.

[14] M. Knapp, Exact values of the function $\Gamma^*(k)$, *J. Number Theory* **131** (2011) 1901-1911.

[15] M. Knapp, Pairs of additive forms of odd degrees, *Michigan Math J.* **61** (2012) 493-505.

[16] M. Knapp, 2-Adic zeros of diagonal forms, *J. Number Theory* **193**(C) (2018) 37-47.

[17] D. J. Lewis, Cubic homogeneous polynomials over p-adic number fields, *Ann. of Math. (2)* **56** (1952) 473-478.

[18] K. K. Norton, On homogeneous diagonal congruences of odd degree, Ph.D. Thesis, University of Illinois, 1966.

[19] A. Tietäväinen, On a Problem of Chowla and Shimura, *J. Number Theory* **3** (1971) 247-252.