Exact Values of the Function $\Gamma^*(k)$

Michael P. Knapp

1. Introduction.

A special case of a conjecture commonly attributed to Artin (see [1]) claimed that any homogeneous additive polynomial

$$a_1x_1^k + a_2x_2^k + \cdots + a_sx_s^k \tag{1}$$

whose coefficients are rational integers should have a nontrivial zero in each p-adic field $\mathbb{Q}_p$ provided only that $s \geq k^2 + 1$. This was verified by Davenport & Lewis [6], who showed further that this bound on s is best possible when $k + 1$ is a prime. That is, they showed that if $k + 1$ is prime, then there exist additive forms in k^2 variables which

Parts of this research were completed and this article was written while the author was enjoying the hospitality of the Universidade de Brasília while on sabbatical leave.

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

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

do not have nontrivial solutions in the $(k+1)$-adic integers. In this paper, Davenport & Lewis defined the function $\Gamma^*(k)$ to represent the smallest number of variables which will guarantee that the form (1) has nontrivial p-adic zeros for every prime p. In this language, Davenport & Lewis showed that $\Gamma^*(k) \leq k^2+1$ for each integer k, and that equality holds whenever $k+1$ is prime.

Since that time, a relatively small amount of effort has been expended on finding other bounds on and values of $\Gamma^*(k)$. Dodson [7] has recorded the bound

$$\Gamma^*(k) \leq \frac{1}{2}k^2\left(1+\frac{2}{1+\sqrt{1+4k}}\right)+1, \quad k \text{ composite.}$$

Another good general bound on $\Gamma^*(k)$ for odd values of k was provided by Tietäväinen [12]. This bound says that for odd k, we have

$$\limsup_{k\to\infty}\frac{\Gamma^*(k)}{k\log k}=\frac{1}{\log 2}.$$

Hence, for any any $\epsilon>0$ and k odd and sufficiently large (depending on ϵ), we have $\Gamma^*(k) < (1+\epsilon)k\log k/\log 2$.

It is somewhat surprising, however, that other than the result of Davenport & Lewis for when $k+1$ is prime, not many exact values of $\Gamma^*(k)$ are known. Classical results on quadratic forms yield $\Gamma^*(2)=5$.

Lewis [10] showed that $\Gamma^*(3) = 7$. Gray [8] showed that additive forms of degree 5 in 16 variables have nontrivial zeros in all p-adic fields except $\mathbb{Q}_5$, and gave an example of an additive form of degree 5 in 15 variables with no 11-adic zeros. Shortly after this, S. Chowla [5] gave a sketch of a method to show that 16 variables suffice over $\mathbb{Q}_5$ as well. Together, this shows that $\Gamma^*(5) = 16$. The values $\Gamma^*(7) = 22$ and $\Gamma^*(11) = 45$ appear to first have been found by Bierstedt [2]. These values were independently discovered by Norton [11], who also gave the value $\Gamma^*(9) = 37$. Dodson also discovered independently the values of $\Gamma^*(7)$ and $\Gamma^*(9)$, stating in [7] that these values can be determined using the results of that paper, although he does not give a proof. Some years later, Bovey [3] showed that $\Gamma^*(8) = 39$. Until recently, these were the only values of $\Gamma^*(k)$ to be known exactly.

While studying an aspect of Artin's conjecture relating to systems of equations [9], the author was led to investigate the values of $\Gamma^*(k)$ for odd values of k. This work involved evaluating $\Gamma^*(k)$ for small odd k, with the following results.

Lemma 1. *The following values of* $\Gamma^*(k)$ *hold:*

$$\begin{aligned} \Gamma^*(13) &= 53 & \Gamma^*(21) &= 106 \\ \Gamma^*(15) &= 61 & \Gamma^*(23) &= 116 \\ \Gamma^*(17) &= 52 & \Gamma^*(25) &= 101. \\ \Gamma^*(19) &= 58 \end{aligned}$$

The purpose of this article is to evaluate all of the remaining values of $\Gamma^*(k)$ for $k \leq 31$, and also to obtain partial information about $\Gamma^*(32)$. We hope that these results will lead to more conjectures on the general behavior of this function and to more formulas for $\Gamma^*(k)$, either for k having specific forms or in general.

In order to state our theorem, we need one more definition. If p is a prime number, then we define the function $\Gamma_p^*(k)$ to be the smallest number of variables required to guarantee that any additive form of degree k with integer coefficients has a nontrivial zero in $\mathbb{Q}_p$. Then the functions $\Gamma^*(k)$ and $\Gamma_p^*(k)$ are related by the formula

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

With this notation, we can now state the main theorem of this article.

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

$$\begin{array}{ll} \Gamma^*(14) = 71 & \Gamma^*(27) = 109 \\ \Gamma^*(20) = 241 & \Gamma^*(29) = 146 \\ \Gamma^*(24) = 289 & \Gamma^*(31) = 125. \\ \Gamma^*(26) = 157 & \end{array}$$

Moreover, we have $\Gamma_p^*(32) \leq 513$ *for all* $p > 2$*, and* $524 \leq \Gamma_2^*(32) \leq 581$*.*

Note that the last part of the theorem implies[1] that $\Gamma^*(32) = \Gamma_2^*(32)$.

For the most part, the proof of this theorem will proceed along the same lines as the proof of Lemma 1 of [9]. For specific k and p, the problem reduces to finding a nonsingular solution of a particular congruence equation. For each degree, we use a result of Dodson [7] to show that the congruence has solutions when p is sufficiently small, and another result found in [7] to show that there are solutions whenever p is sufficiently large. In general, the remaining primes are divided into two groups. The primes p such that $p \nmid k$ and $p \not\equiv 1 \pmod{k}$ can usually be treated fairly quickly using the theory of k-th power residues modulo primes. The remaining primes are dealt with computationally

[1]Since this research was completed, we have managed to show that $\Gamma_2^*(32) = 524$, and hence that $\Gamma^*(32) = 524$. Unfortunately, the proof of this fact is too long to be included here, and will be deferred to a future article.

in two ways. First, a method due to Bovey [3] involving exponential sums is used to show that the congruence equation has solutions for the majority of these primes. For the few primes that are resistant to this method, we essentially check every possible choice of coefficients and make certain that the required congruence equation always has solutions.

We note here that Bovey's method was not used while proving the lemma in [9], and represents a significant computational improvement. This is because checking a particular pair of k and p via Bovey's method is much faster than checking the same pair by testing every possible congruence. The slight drawback of Bovey's method is that it can not be used to show that our proposed value of $\Gamma^*(k)$ does not suffice for a given prime. Thus, as mentioned above, the primes for which Bovey's method fails must still be checked by a brute-force computation.

Finally, we mention that for a small number of pairs of k and p, we deviate from the method above. We do this at various points when it seems that the brute-force approach will take a long time, and we are able to give a theoretical argument instead. Most notably, we do this when we have $(k, p) = (27, 3)$ and to deal with 2-adic solubility when

k is even.

In Section 2 of this article, we give the preliminaries necessary to complete the proof of the theorem. While the techniques used are essentially the same for each degree k, the details are different in each case. Thus, in Section 3 we give a complete proof that $\Gamma^*(14) = 71$, and in Section 4 we show how the details change for the other values of k. Finally, since the proof of the case $(k, p) = (27, 3)$ is significantly different from the rest, we treat this one case separately in Section 5.

2. Preliminary Lemmata

In this section, we introduce the tools that we will use to evaluate each of the values of $\Gamma^*(k)$. Our first preliminary lemma, due to Davenport & Lewis [6], shows that we can assume that our forms have certain nice properties. In particular, we can assume that there are many variables that appear with a nonzero coefficient when the form is reduced modulo powers of p.

Lemma 2. *By a nonsingular change of variables of the form $x_i = l_i x_i'$, any additive form as in* (1) *can be transformed into one of the type*

$$F = F_0 + pF_1 + \cdots + p^{k-1}F_{k-1},$$

where each F_i is an additive form in m_i variables, and the variables in each F_i are distinct. Moreover, each variable in each F_i appears with a coefficient which is nonzero modulo p, and for $1 \leq i \leq k$, we have

$$m_0 + m_1 + \cdots + m_{i-1} \geq is/k.$$

For $0 \leq i \leq k-1$, we will say that the variables involved in the form F_i are at *level i*. In practice, we will only be interested in the variables at level 0 and occasionally the variables at level 1.

The next lemma is a version of Hensel's lemma, which tells us that we can lift solutions of congruences to p-adic solutions of equations.

Lemma 3. *Suppose that we wish to solve an equation of the form*

$$a_1 x_1^k + \cdots + a_s x_s^k = 0 \tag{2}$$

over the ring $\mathbb{Z}_p$. Write $k = k_0 p^\tau$ with $(k_0, p) = 1$, and define the number γ by

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

If we can find a solution of the congruence

$$a_1 x_1^k + \cdots + a_s x_s^k \equiv 0 \pmod{p^\gamma}$$

such that at least one variable at level 0 is relatively prime to p, then this solution lifts to a solution of (2).

If a solution of a congruence has the property described in this lemma, then we will call it a *nonsingular* solution. When we use this lemma, we will typically assume that all of the variables are at level 0, so that any nontrivial solution is nonsingular.

We now state several results which we will use to guarantee that certain congruences have nontrivial solutions. The first of these is a trivial consequence of (the proof of) Lemma 2.4.1 of [7].

Lemma 4. *Consider the congruence*

$$a_1 x_1^k + \cdots + a_t x_t^k \equiv 0 \pmod{p}. \tag{3}$$

If p does not divide either k or any of the coefficients a_i, then the congruence (3) *has a nonsingular solution whenever we have*

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

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

Our second lemma for solving congruences is due to Dodson, and is essentially the first part of Lemma 3.2.1 of [7].

Lemma 5. *Consider the congruence*

$$a_1x_1^k + \cdots + a_tx_t^k \equiv 0 \pmod{p^\gamma}. \tag{4}$$

If -1 is a k-th power residue modulo p^γ, and p does not divide any of the coefficients a_i, then the congruence (4) *has a nonsingular solution whenever $2^t > p^\gamma$.*

Note that the equation (3) is just the special case $\gamma = 1$ of (4). For the sake of uniformity, in situations where $\gamma = 1$ we will frequently refer to equation (4) instead of equation (3), using this fact implicitly.

Our next lemma is the well-known Chevalley's theorem [4]. While this theorem of course can be extended to systems of equations of any degrees, we only state a form of it that we will need.

Lemma 6. *Suppose that $f(x_1, \ldots, x_t)$ 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 $\mathbb{F}_p$.*

Our last lemma about congruences is essentially due to Bovey, and is similar to Lemma 1 of [3]. Although Bovey only states this lemma for congruences modulo 2^N, one can replace the prime 2 in his proof by any prime p, and the proof still works. After doing this, we obtain the following lemma.

Lemma 7. *Let n be a positive integer and suppose that for $i = 0, \ldots, n$, we have $F_i = \sum_{j=1}^{m_i} a_{ij} x_{ij}$ with $p \nmid a_{ij}$ for all i, j and with $\sum_{i=0}^{l-1} m_i \geq p^l$ for each $l = 1, \ldots, n$. Then for any positive integer $N > n$, the form $\sum_{i=0}^{n} p^i F_i$ represents at least $\min\left\{\sum_{i=0}^{n} m_i, p^N\right\}$ different residue classes modulo p^N, where the x_{ij} are either 0 or 1, and with at least one of the $x_{0j} = 1$.*

Our final lemma in this section is also due to Bovey, and is essentially Lemma 5 of [3], although it also incorporates some of the remarks preceding that lemma.

Lemma 8. *Suppose that positive integers k, p, t are given, with p prime and $p \nmid k$, and consider the congruence (3), where all of the coefficients are relatively prime to p. Define the function $Q(k, p, t)$ by*

$$Q(k, p, t) = \sum_{b=1}^{p-1} |S(b)|^t / (p^t - p),$$

where we have

$$S(b) = \sum_{x=0}^{p-1} e_p(bx^k), \qquad \text{and} \qquad e_p(x) = e^{2\pi i x/p}.$$

If $Q(k, p, t) < 1$, then we have $\Gamma^*(k) \leq k(t-1) + 1$.

We end this section with a description of our strategy for verifying that our theorem holds for a particular degree k and prime p by essentially testing every possible congruence (4). This strategy is similar to the one used by Bierstedt in [2]. We seek to economize the time required by limiting the number of individual congruences for which we need to compute solutions. For the moment, assume that $p \nmid k$, so that none of the coefficients in (4) are divisible by p, and observe that by dividing the entire congruence by a_1, we may assume that $a_1 \equiv 1 \pmod{p^\gamma}$.

Next, suppose that (4) has a nonsingular solution $\mathbf{x} = \mathbf{z}$ for some specific choice of coefficients $a_1, \ldots, a_t$, and let b_i, ζ_i be numbers nonzero modulo p such that

$$b_i \equiv \zeta_i^k \cdot a_i \pmod{p^\gamma}, \qquad (1 \leq i \leq t).$$

Then we can see that the congruence

$$b_1 x_1^k + \cdots + b_t x_t^k \equiv 0 \pmod{p^\gamma}$$

has a nonsingular solution by simply setting $x_i \equiv z_i/\zeta_i \pmod{p^\gamma}$. Hence, for each coset of $(\mathbb{Z}/p^\gamma\mathbb{Z})^\times/(\mathbb{Z}/p^\gamma\mathbb{Z})^{\times k}$, 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 (4) as a coefficient. Moreover, if k is odd and we can write $a_i \equiv \zeta^k a_j \pmod{p^\gamma}$ for some indices i, j, then we can get a nonsingular solution of (4) by setting $x_i = -1, x_j = \zeta$, and all other variables equal to 0. Thus, when k is odd we may assume that different coefficients in (4) come from different cosets.

In light of these observations, we use the following strategy in our calculations. Noting that $(\mathbb{Z}/p^\gamma\mathbb{Z})^\times/(\mathbb{Z}/p^\gamma\mathbb{Z})^{\times k}$ is cyclic, we first find a number g such that the set $\{1, g, g^2, \ldots, g^{k-1}\}$ contains one representative of each coset of $(\mathbb{Z}/p^\gamma\mathbb{Z})^\times/(\mathbb{Z}/p^\gamma\mathbb{Z})^{\times k}$. Hence we may assume that $a_1 = 1$ and that $(a_2, \ldots, a_t) = (g^{c_2}, \ldots, g^{c_t})$, where we have $1 \leq c_2 \leq c_3 \leq \cdots \leq c_t \leq k-1$. (If k is odd, then all of these inequalities except the first and last may be replaced by strict inequalities.) This greatly reduces the number of congruences that need to be solved. Each of these congruences is solved by a brute-force approach, using MAPLE to systematically test all possible combinations of k-th powers until a solution is found.

If it happens that $p|k$, then we first attempt to solve (4) using only the variables which are guaranteed by Lemma 2 to be in F_0, having coefficients which are not divisible by p. For these variables, everything works exactly as above. If it turns out that these variables by themselves are not enough to guarantee that (4) has solutions for all choices of coefficients, then we add one more variable, which may lie in either F_0 or F_1, and solve the resulting congruence by brute force. This new variable may or may not have a coefficient divisible by p, but will not have a coefficient divisible by p^2. We will see that the s/k variables guaranteed to have coefficients not divisible by p plus one more variable will always suffice to guarantee that (4) has nonsingular solutions.

3. The Proof that $\Gamma^*(14) = 71$

Consider the congruence

$$G(\mathbf{x}) = x_1^{14} + 16x_2^{14} + 16x_3^{14} + 41x_4^{14} + 41x_5^{14} \equiv 0 \pmod{43}.$$

It can be verified computationally that the only solution of this congruence is $\mathbf{x} \equiv \mathbf{0} \pmod{43}$. Thus one can see that the equation

$$G(\mathbf{x_1}) + 43 \cdot G(\mathbf{x_2}) + \cdots + 43^{13} \cdot G(\mathbf{x_{14}}) = 0$$

has no nontrivial 43-adic solutions, where $\mathbf{x_1}, \mathbf{x_2}, \ldots$ represent disjoint sets of variables $\mathbf{x_i} = (x_{i1}, \ldots, x_{i5})$. Since this equation has 70 variables and no nontrivial 43-adic solutions, we must clearly have $\Gamma^*_{43}(14) \geq 71$, and hence $\Gamma^*(14) \geq 71$.

Next, assume that $s \geq 71$, and for any prime p, define $\gamma = \gamma(k, p)$ as in Lemma 3. Our goal will be to solve the equation (4) using only the variables at level 0. By Lemma 2, we may assume that there are (at least) 6 such variables. First, note that if $p > 14$, then we certainly have $\gamma = 1$, and so (4) is just an equation modulo p, as in (3). Thus we can apply Lemma 4 with $t = 6$ and $k = 14$, finding that we can solve the congruence (4) nontrivially (and hence nonsingularly) whenever we have

$$p > 13^{10/4} \approx 609.34.$$

Similarly, we may apply Lemma 5 with $t = 6$, and we find that the congruence (4) has nontrivial solutions whenever -1 is a 14th power modulo p^γ and also

$$p^\gamma < 2^6 = 64.$$

Considering only odd primes for the moment and noting that -1 is always a 7th power modulo p, we see that -1 is a 14th power modulo p if and only if it is a perfect square modulo p, ie. if and only if $p \equiv 1 \pmod 4$. Thus we see that (4) has nontrivial solutions whenever we have $p = 5, 13, 17, 29, 37, 41, 53,$ or 61.

Suppose next that p is a prime such that $p \nmid 14$ and $(14, p-1) = 2$. Then it is well-known that the set of 14th powers modulo p is the same as the set of squares modulo p. Hence the congruence (4) will have solutions if and only if the congruence

$$a_1 x_1^2 + \cdots + a_6 x_6^2 \equiv 0 \pmod{p}$$

does. Since this is an equation of degree 2 in more than two variables, Lemma 6 tells us that this congruence has nontrivial solutions. Because $p-1$ must be even, we see that $(14, p-1) \in \{2, 14\}$, and hence the congruence (4) has nontrivial solutions whenever $\gamma = 1$ and $(14, p-1) \neq 14$, (ie. when $p \not\equiv 1 \pmod{14}$). For all of the primes we have dealt with so far, we have seen that (4) has nonsingular solutions, and hence Lemma 3 shows that (2) has nontrivial p-adic solutions. Hence $\Gamma_p^*(14) \leq 71$ for these primes.

We now use Lemma 8 to begin the computational study of the remaining primes with $p \equiv 1 \pmod{14}$. In order to show that $\Gamma_p^*(14) \leq 71$ for a prime p via this lemma, we need to have $Q(14, p, 6) < 1$. In fact, we do a little bit better by computing $Q(14, p, 5)$. If this quantity is less than 1, we will actually know that $\Gamma_p^*(14) \leq 57$ for these primes. When we perform our calculations using MAPLE, we obtain the values in the table below, rounded to five decimal places.

p	$Q(14, p, 6)$	p	$Q(14, p, 6)$	p	$Q(14, p, 6)$
43	4.80804	211	0.71988	421	0.26367
71	2.23892	239	0.83546	449	0.53405
113	1.95433	281	0.77894	463	0.12468
127	1.26087	337	0.43891	491	0.15717
197	0.74873	379	0.40432	547	0.08624

Thus the only primes with $p \nmid 14$ which we still need to check are 43, 71, 113, and 127. We deal with these by the "brute force" method described after the lemmas in the previous section. As with our previous computations, we assume for now that we only have 5 variables at level 0, and here MAPLE shows that all possible congruences of the form (4) have nontrivial solutions when $p = 71, 113$, and 127. Since there are only 5 variables at level 0, we see that $\Gamma_p^*(14) \leq 57$ for these primes as well. To deal with $p = 43$, we add a sixth variable at level 0, and MAPLE shows that now all possible equations of the form (4) have solutions. Hence we have $\Gamma_{43}^*(14) \leq 71$, and in fact the remarks at the beginning of this subsection now show that $\Gamma_{43}^*(14) = 71$.

Finally, we need to deal with the primes $p = 2$ and $p = 7$, which divide 14. For the prime $p = 7$, we again use our brute-force approach. This time, we have $\gamma = 2$, and so we need to look at congruences modulo $7^2 = 49$. As before, we know that we have at least 6 variables at level 0. Thus we begin by testing to see whether every congruence modulo 49 involving only 6 variables at level 0 has a nonsingular solution. MAPLE shows that this is indeed the case. Since all of these nonsingular solutions lift to 7-adic solutions, we see that $\Gamma_7^*(14) \leq 71$.

Finally, to handle the prime $p = 2$, we use Lemma 7. When $k = 14$ and $p = 2$, we have $\tau = 1$ and $\gamma = 3$. Thus we need to find a nonsingular solution of (4), where the congruence is modulo 2^3. Now, from Lemma 2, since our form has 71 variables, we have

$$\begin{array}{rcccl} m_0 & \geq & 6 & \geq & 2^1 \\ m_0 + m_1 & \geq & 11 & \geq & 2^2 \\ m_0 + m_1 + m_2 & \geq & 16 & \geq & 2^3, \end{array}$$

and hence Lemma 7 guarantees that the variables at levels 0, 1, and 2 together represent each residue class modulo 8 with at least one variable at level 0 not divisible by 2. In particular, these variables represent the zero residue nonsingularly, and hence Lemma 3 guarantees that the equation (2) has a nontrivial solution in $\mathbb{Z}_p$.

4. The Other Values of k

In this section, we show how to prove the theorem for other values of k. For the most part, we will work on all the other values at the same time, and will just give an outline where the steps are essentially identical to the steps for $k = 14$. In this section, all variables except p are understood to be functions of k, although this will typically not be explicitly shown.

We begin by proving the theorem for the primes such that $p \nmid k$. When $k = 20$, we will go a little further than in the statement of the theorem and show that when $p \nmid 20$, having only 201 variables suffices to guarantee p-adic solubility. For each value of k, we begin by calculating the minimum number t of variables which are guaranteed to be at level 0 when (2) has at least the number of variables in the theorem. These values are in the table below. For each prime p, the congruence (4) is equivalent to one of degree $d = (k, p-1)$, and we attempt to use Lemma 6 to show that this congruence has a nonsingular solution. For each value of k except 27, this allows us to assume that $d = k$, ie. that $p \equiv 1 \pmod{k}$. When $k = 27$, we still need to consider both the cases $d = 9$ and $d = 27$.

Next, we use Lemma 4 to calculate a bound p_0 such that we know that the theorem is true for additive forms of degree k whenever $p > p_0$. (When $k = 27$, since the equation (4) is equivalent to one of degree either 9 or 27, we use Lemma 4 twice, taking each of these as the degree.) Then, when it is easy to determine whether -1 is a k-th power modulo p, we use Lemma 5 to show that (4) has nonsingular solutions for certain small primes. The results of this work are in the table below.

k	t	Bound from Lemma 4	Bound from Lemma 5
20	11	$p \geq 695$	
24	13	$p \geq 936$	
26	7	$p \geq 2265$	
27	5	$p > 256$ when $(27, p-1) = 9$ $p > 5933$ when $(27, p-1) = 27$	$p < 32$ and $p \neq 3$
29	6	$p > 4149$	$p < 64$ and $p \neq 29$
31	5	$p > 8690$	$p < 32$ and $p \neq 31$
32	17	$p > 1520$	

Next, for each of the remaining primes, we calculate the value of $Q(d, p, t)$. As before, if $Q(d, p, t) < 1$, then we know that our bound holds for this value of p, but the primes with $Q(d, p, t) \geq 1$ need further study. We will not give all the values of $Q(d, p, t)$ here, but we do list the primes with $Q(d, p, t) \geq 1$ in the table below. We can check by brute force that each possible diagonal form of degree k in t variables has a nonsingular solution modulo p for each of these exceptional primes. When we do this, MAPLE verifies that these solutions do exist. Hence the theorem is true for all primes with $p \nmid k$. In some cases, we saved some computing time by using fewer than t variables, and MAPLE showed that having fewer variables at level 0 was sufficient to guarantee nonsingular solutions modulo p. This leads to smaller bounds on $\Gamma_p^*(k)$ for these primes, and the bounds we obtained are also in the table below.

k	Exceptional Primes with $Q(d,p,t) > 1$	Bound on $\Gamma_p^*(k)$
20	41, 61	101
24	73, 97	121
26	53, 131, 157	131
	79	157
27	37 when $(27, p-1) = 9$	109
	109, 163, 271, 379, 433, 487, 541 when $(27, p-1) = 27$	109
29	59, 233, 349	146
31	311, 373, 683	125
32	97, 193	193

For the primes dividing k, we are typically able to use an argument similar to the one used to treat the prime 2 in the previous section.

For example, when $k = 20$ and $p = 5$ (and remembering that we are now allowing 241 variables over $\mathbb{Z}_5$), Lemma 2 yields

$$\begin{aligned} m_0 \quad &\geq \ 13 \ \geq \ 5^1 \\ m_0 + m_1 &\geq \ 25 \ \geq \ 5^2. \end{aligned}$$

Thus Lemma 7 shows that (4) has a solution with at least one nonzero variable at level 0. This solution is nonsingular, and hence (2) has nontrivial zeros. This method works when the ordered pair (k, p) is any of $(20, 2)$, $(20, 5)$, $(24, 2)$, $(24, 3)$, $(26, 2)$, or $(32, 2)$. (Remember that for the $k = 32$ case we are now allowing 581 variables over $\mathbb{Z}_2$.) For the ordered pairs $(26, 13)$, $(29, 29)$, and $(31, 31)$, this argument fails, and so we test equations by brute force. In the first two cases, we find that having 6 variables at level 0 is enough to guarantee that the equation (4) has a nontrivial solution modulo p^2, and in the last case, 5 variables at level 0 are sufficient. The final possibility is $(k, p) = (27, 3)$. We treat this case theoretically, but the argument is a bit long, and so we defer it to the next section.

At this point, we have shown that the values in the theorem are all upper bounds for $\Gamma^*(k)$. To show that they are exact values, we must find a prime p and a form in one fewer variable which has no p-adic zeros. For most of the degrees under consideration, this is done exactly as in the previous section. The table below contains the special prime for each degree and an example of a form which has no nontrivial zeros modulo p. These forms can then be extended as in the previous section to forms with no p-adic zeros.

k	p	Form Modulo p
24	13	$x_1^{24} + x_2^{24} + \cdots + x_{12}^{24}$
26	79	$x_1^{26} + x_2^{26} + 3x_3^{26} + 3x_4^{26} + 54x_5^{26} + 54x_6^{26}$
27	19	$x_1^{27} + 2x_2^{27} + 4x_3^{27} + 8x_4^{27}$
29	59	$x_1^{29} + 2x_2^{29} + 4x_3^{29} + 8x_4^{29} + 16x_5^{29}$
31	311	$x_1^{31} + 2x_2^{31} + 10x_3^{31} + 32x_4^{31}$

We treat the degrees 20 and 32 slightly differently. For degree 20, since 1 is the only nonzero 20th power modulo 25, the congruence

$$G(\mathbf{x}) = x_1^{20} + x_2^{20} + \cdots + x_{24}^{20} \equiv 0 \pmod{25}$$

has no primitive solutions (ie. no solutions with any variable not divisible by 5). Thus the equation

$$G(\mathbf{x_0}) + 5^2 \cdot G(\mathbf{x_1}) + 5^4 \cdot G(\mathbf{x_2}) + \cdots + 5^{18} \cdot G(\mathbf{x_9}) = 0$$

has no nontrivial 5-adic solutions. Similarly, for degree 32, note that 1 is the only nonzero 32nd power modulo 2^7. Thus the congruence

$$G(\mathbf{x}) = x_1^{32} + x_2^{32} + \cdots + x_{127}^{32} \equiv 0 \pmod{2^7}$$

has no primitive solutions. One can then see that the equation

$$G(\mathbf{x_0}) + 2^7 \cdot G(\mathbf{x_1}) + 2^{14} \cdot G(\mathbf{x_2}) + 2^{21} \cdot G(\mathbf{x_3}) + 2^{28} \cdot \sum_{i=1}^{15} y_i^{32} = 0$$

has no nontrivial 2-adic solutions. Except for the one remaining case when $k = 27$ and $p = 3$, this completes the proof of the theorem.

5. The Proof when $k = 27$ and $p = 3$

In this final section, we complete the proof of the theorem by showing that $\Gamma_3^*(27) \leq 109$. In this case, we have $\tau = 3$, and hence (4) is a congruence modulo 81. Note that Lemma 2 yields

$$\begin{array}{rcccl} m_0 & \geq & 5 & \geq & 3^1 \\ m_0 + m_1 & \geq & 9 & \geq & 3^2. \end{array}$$

Suppose first that we have $m_0 \geq 7$. Then Lemma 5 shows that a nonsingular solution of (4) exists, using only the variables at level 0. If we have $m_0 = 6$, then an argument analogous to the proof given in [7] of Lemma 5 shows that (4), using the variables at level 0 and one variable from level 1, possesses a nontrivial solution. Since such a solution must have at least two nonzero variables, there must be a nonzero variable at level 0, and hence this solution is also nonsingular. Thus we may assume that $m_0 = 5$, and hence that $m_1 \geq 4$. That is, we may assume that (4) looks like

$$a_1x_1^{27} + \cdots + a_5x_5^{27} + 3\left(b_1y_1^{27} + \cdots + b_4y_4^{27}\right) \equiv 0 \pmod{81},$$

where $a_1 \ldots, a_5, b_1, \ldots, b_4$ are all nonzero modulo 3.

If it happens that there exist indices i, j such that the equation

$$3\left(b_iy_i^{27} + b_jy_j^{27}\right) \equiv 0 \pmod{81} \tag{5}$$

has no solutions, then we can consider only these two y-variables along with all the variables at level 0. Since there are a total of 7 variables, (4) has a nontrivial solution as in the $m_0 = 6$ case above, and since the solution cannot involve only the two y-variables, this solution must be nonsingular. Thus we may assume that (5) has a nontrivial solution for any two indices i, j. Since the only 27th powers modulo 81 are 1 and -1, we see that for each i, j, we must have either

$$b_i \equiv b_j \pmod{27} \qquad \text{or} \qquad b_i \equiv -b_j \pmod{27}.$$

Now we show that under these conditions, there must exist indices i, j such that one of the congruences

$$b_i \equiv b_j \pmod{81} \qquad \text{or} \qquad b_i \equiv -b_j \pmod{81} \tag{6}$$

holds. Once this is known, Lemma 3 shows that the equation $b_i y_i^{27} \pm b_j y_j^{27} = 0$ has a nontrivial 3-adic solution, and hence that (2) has one also. To see that one of the congruences in (6) holds, first consider the case where all of the b_i are congruent modulo 27. Then by the pigeonhole principle, two of them must be congruent modulo 81, and we are done.

Next, suppose that exactly three of the b_i are congruent modulo 27. Without loss of generality, we can assume that

$$b_1 \equiv b_2 \equiv b_3 \equiv -b_4 \pmod{27}.$$

If none of b_1, b_2, b_3 are congruent modulo 81, then we have $\{b_2, b_3\} \equiv \{b_1 + 27, b_1 + 54\} \pmod{81}$. But then we must have $b_4 \equiv -b_i \pmod{81}$ for some $i \in \{1, 2, 3\}$, and again we find a solution of (6).

Finally, we consider the case where no three of the b_i are congruent modulo 27. In this case, we may assume without loss of generality that

$$b_1 \equiv b_2 \equiv -b_3 \equiv -b_4 \pmod{27}.$$

Hence we can write

$$\begin{aligned} b_2 &\equiv b_1 + 27c_2 \pmod{81} \\ b_3 &\equiv -b_1 + 27c_3 \pmod{81} \\ b_4 &\equiv -b_1 + 27c_4 \pmod{81}, \end{aligned}$$

with $c_2, c_3, c_4 \in \{0, 1, 2\}$. Now, if $b_1 + b_3$ and $b_1 + b_4$ are both nonzero modulo 81, then we see that $c_3, c_4 \neq 0$. If in addition $b_3 \not\equiv b_4 \pmod{81}$, then we have $\{c_3, c_4\} = \{1, 2\}$. Moreover, if $b_1 \not\equiv b_2 \pmod{81}$, then we have $c_2 \in \{1, 2\}$. Suppose without loss of generality that $c_2 \neq c_3$. Then $\{c_2, c_3\} = \{1, 2\}$ and we have

$$b_3 = -b_2 + 27(c_2 + c_3) \equiv -b_2 \pmod{81},$$

and so again (6) has a solution. Thus we have seen that in any of the possible cases, we can always find a nontrivial solution of (2), and hence $\Gamma_3^*(27) \leq 109$.

References

1. E. Artin, *Collected papers*, Addison-Wesley Pub. Co., Reading, Mass., 1965.

2. R. G. Bierstedt, *Some problems on the distribution of kth power residues modulo a prime*, Ph.D. thesis, University of Colorado, 1963.
3. J. D. Bovey, *"$\Gamma^*(8)$"*, Acta Arith. **25** (1974), 145–150.
4. C. Chevalley, *"Démonstration d'une hypothèse de M. Artin"*, Abh. Math. Sem. Hamburg **11** (1935), 73–75.
5. S. Chowla, *"On a conjecture of J. F. Gray"*, Norske Vid. Selsk. Forh. Trondheim **33** (1960), 58–59.
6. H. Davenport and D. J. Lewis, *"Homogeneous additive equations"*, Proc. Royal Soc. London Ser. A **274** (1963), 443–460.
7. M. Dodson, *"Homogeneous additive congruences"*, Philos. Trans. Roy. Soc. London Ser. A **261** (1967), 163–210.
8. J. F. Gray, *Diagonal forms of prime degree*, Ph.D. thesis, University of Notre Dame, 1958.
9. M. Knapp, *"Pairs of additive forms of odd degree"*, (submitted).
10. D. J. Lewis, *"Cubic congruences"*, Michigan Math. J. **4** (1957), 85–95.
11. K. K. Norton, *On homogeneous diagonal congruences of odd degree*, Ph.D. thesis, University of Illinois, 1966.
12. 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