Michigan Math. J. 69 (2020), 533–543

Infinitely Many Counterexamples to a Conjecture of Norton

Hemar Godinho & Michael P. Knapp

Abstract. For any positive integer k, we define $\Gamma^*(k)$ to be the smallest number s such that every diagonal form $a_1x_1^k + a_2x_2^k + \cdots + a_sx_s^k$ in s variables with integer coefficients must have a nontrivial zero in every p-adic field $\mathbb{Q}_p$. An old conjecture of Norton is that we should have $\Gamma^*(k) \equiv 1 \pmod{k}$ for all k. For many years, $\Gamma^*(8) = 39$ was the only known counterexample to this conjecture, and in recent years two more counterexamples have been found. In this article, we produce infinitely many counterexamples to Norton's conjecture.

1. Introduction

In this article, we study p-adic zeros of diagonal forms with (rational) integer coefficients. Specifically, let k be a positive integer and define the diagonal form F by

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

where a_i are all rational integers. If p is a prime, then $\Gamma^*(k, p)$ is defined to be the smallest value of s such that F is guaranteed to have nontrivial p-adic zeros regardless of the values of the coefficients. Moreover, the function $\Gamma^*(k)$ is defined by

$$\Gamma^*(k) = \max_{p \text{ prime}} \Gamma^*(k, p). \tag{2}$$

Thus, $\Gamma^*(k)$ is the smallest value of s, which guarantees that F has nontrivial zeros in every p-adic field $\mathbb{Q}_p$.

An old result of Davenport and Lewis [4] is the bound $\Gamma^*(k) \le k^2 + 1$, with equality whenever $k + 1$ is a prime. After this result, several authors (see [1; 5; 10]) began calculating the exact values of $\Gamma^*(k)$ for small degrees k. For these k, we have $\Gamma^*(k) \equiv 1 \pmod{k}$, and Norton conjectured in his PhD thesis [10] that this congruence should hold for all k. This conjecture was disproved by Bovey [2], who showed that $\Gamma^*(8) = 39$. For many years, this was the only known counterexample until Knapp [8; 9] showed that $\Gamma^*(32) = 524$. More recently, Veras et al. [7] and Jennings (unpublished) independently showed that $\Gamma^*(54) = 1049$, giving a third counterexample. In this article, our main goal is to produce infinitely many counterexamples to Norton's conjecture. In particular, we prove the following theorem.

Received June 20, 2018. Revision received December 5, 2018.

THEOREM 1. *Let $\tau \geq 2$ be an integer. Then there are infinitely many primes q such that if we set $k = q^\tau(q-1)$, then $\Gamma^*(k) \not\equiv 1 \pmod{k}$.*

In order to prove this theorem, we work with primes q of a special form, which we now define. Suppose that $\tau \geq 2$ is given, and let

$$7 = p_1 < p_2 < \cdots < p_t \leq \tau + 1$$

be all the odd primes, if any exist, in the interval $[7, \tau+1]$. If $\tau < 6$, then p_i are undefined or, if the reader prefers, we can take $p_1 = \cdots = p_t = 1$ in the arguments involving p_i. We say that a prime q satisfies **Condition C(τ)** if all of the following are true:

1. $q \equiv 3 \pmod{4}$.
2. $q \equiv 2 \pmod{p}$ for $p \in \{3, 5, p_1, \ldots, p_t\}$.
3. $q > \tau + 1$.
4. Writing $k = q^\tau(q-1)$, we have $k^{1/8}/(\log k)^2 > 12(\tau+1)$.

With this definition, we prove the following theorem.

THEOREM 2. *Let $\tau \geq 2$ be an integer. If τ is not divisible by 4, then we have*

$$\Gamma^*(k) = \Gamma^*(k, q) \not\equiv 1 \pmod{k} \tag{3}$$

for every prime q satisfying Condition C(τ) and degree $k = q^\tau(q-1)$. If τ is divisible by 4, then (3) is true for infinitely many primes satisfying Condition C(τ).

We note that Theorem 2 immediately implies Theorem 1. The congruences in Condition C(τ) are equivalent to a single congruence of the form $q \equiv A \pmod{60 p_1 \cdots p_t}$ for some number A relatively prime to $60 p_1 \cdots p_t$. Dirichlet's theorem on primes in arithmetic progressions guarantees that there are infinitely many primes q that will satisfy this congruence. Then the last part of Condition C(τ) will hold whenever q is sufficiently large.

We are also able to produce new families of k-values such that $\Gamma^*(k) \equiv 1 \pmod{k}$. Suppose that $\tau + 1$ is prime, and observe that in this case we have $p_t = \tau + 1$. We say that a prime q satisfies **Condition D(τ)** if it satisfies all the parts of Condition C(τ), except that we now require $q \equiv 1 \pmod{\tau+1}$. Then we have the following theorem.

THEOREM 3. *Let $\tau \geq 2$ be an integer such that $\tau + 1$ is prime, let q be a prime satisfying Condition D(τ), and set $k = q^\tau(q-1)$. If τ is divisible by 4, then assume additionally that $k+1$ is composite. Then we have*

$$\Gamma^*(k) = \Gamma^*(k, q) \equiv 1 \pmod{k}.$$

For each value of k in this theorem, we are determining the value of $\Gamma^*(k)$ for the first time.

We end this section with a few remarks on the quality of these results. Although the condition $k^{1/8}/(\log k)^2 > 12(\tau+1)$ is onerous for small values of τ

(for example, with $\tau = 2$ we need approximately $q > 7.6 \times 10^{14}$), it quickly becomes more manageable as τ increases. In fact, if $\tau \geq 125$, then any odd prime will guarantee that this condition is fulfilled.

The condition $q > \tau + 1$ in Theorems 2 and 3 is also very mild. The systems of congruence conditions in Conditions C(τ) and D(τ) each reduces to a single congruence modulo $60p_1p_2\cdots p_t > \tau + 1$. Hence there is at most a single prime $q \leq \tau + 1$ that satisfies the congruences and is excluded by this condition.

We should mention that we have chosen most of our congruence conditions for convenience rather than out of necessity. If we replace the congruences $q \equiv 2 \pmod{p_i}$ in the definition of Condition C(τ) by $q \equiv c_i \pmod{p_i}$, where $2 \leq c_i \leq p_i - 1$ are integers fixed in advance, then Theorem 2 will still hold.

Finally, we note that every counterexample to Norton's conjecture that we produce in this article is even. It is unknown whether it is possible to have $\Gamma^*(k) \not\equiv 1 \pmod{k}$ when k is odd.

2. Preliminaries

In this section, we give the preliminary results and concepts that we need to prove our theorems. Our goal is to prove that $\Gamma^*(k, p) \leq \Gamma^*(k, q)$ for all primes $p \neq q$. This, in light of (2), immediately leads to $\Gamma^*(k) = \Gamma^*(k, q)$. We find the exact value of $\Gamma^*(k, q)$ through the following lemma. The $p = 2$ case of the lemma is the main result of [9], whereas the general case is part of [7, Theorem 1].

LEMMA 4. *Let k be an integer, and let p be a prime such that $p - 1$ divides k. Write $k = p^\tau k_0$ with $p \nmid k_0$, and define the number γ by*

$$\gamma = \gamma(k, p) = \begin{cases} \tau + 2 & \text{if } p = 2 \text{ and } \tau \geq 1, \\ \tau + 1 & \text{otherwise.} \end{cases} \tag{4}$$

Further, write $k = \gamma q + r$ with $0 \leq r \leq \gamma - 1$. Then we have

$$\Gamma^*(k, p) = (p^\gamma - 1)q + p^r = (p^\gamma - 1)\left(\frac{k - r}{\gamma}\right) + p^r.$$

Suppose now that F is an additive form as in (1) in $s = \Gamma^*(k, q)$ variables. If $p \neq q$, then we will prove that $\Gamma^*(k, p) \leq \Gamma^*(k, q)$ by showing that F must have a p-adic zero. The following lemmas give us some notation and methods for doing this. The next lemma summarizes several results from [4].

LEMMA 5. *Suppose that F is an additive form as in (1) with (rational) integer coefficients, and let p be a prime. If we wish to prove that F has a nontrivial p-adic zero regardless of the coefficients, then it suffices to prove this result for forms with the following properties. We need only consider the forms that can be written as*

$$F = F_0 + pF_1 + p^2F_2 + \cdots + p^{k-1}F_{k-1},$$

where $F_0, \ldots, F_{k-1}$ are additive forms in distinct variables, and every coefficient in each form F_i is relatively prime to p. Moreover, if we write v_i to represent the

number of variables in the form F_i, then we may assume that

$$v_0 + \cdots + v_{j-1} \geq js/k$$

for $1 \leq j \leq k$.

Our next lemma is a standard version of Hensel's lemma. This lemma is [4, Lemma 4], in which it is stated that the lemma follows easily from [12, Chapter 2, Lemma 8].

LEMMA 6. *Suppose that F is a form as in (1), and define the number γ as in (4). Suppose that $\mathbf{x} = (x_1, \ldots, x_s)$ satisfies $F(\mathbf{x}) \equiv 0 \pmod{p^\gamma}$ and that there exists j such that neither a_j nor x_j is divisible by p. Then the form F has a nontrivial p-adic zero.*

The next three lemmas give conditions under which we can guarantee that we can find solutions of congruences of the type $F \equiv 0 \pmod{p^\gamma}$. These lemmas can each be immediately combined with Hensel's lemma to show that F has a p-adic zero. Our next lemma is Chevalley's well-known theorem [3].

LEMMA 7 (Chevalley). *Let p be a prime, and consider the congruence*

$$a_1 x_1^k + \cdots + a_t x_t^k \equiv 0 \pmod{p}, \tag{5}$$

where none of $a_1, \ldots, a_t$ are divisible by p. If $t > k$, then this congruence has a solution with at least one variable nonzero modulo p.

The next lemma is a slightly specialized version of [5, Lemma 2.6.7].

LEMMA 8. *Let p be a prime, and consider congruence (5), where $k|(p-1)$ and $k \neq p-1$, and none of $a_1, \ldots, a_t$ are divisible by p. If $t \geq 12k^{7/8}(\log k)^2$, then the congruence has a solution with at least one variable nonzero modulo p.*

The next lemma is [8, Lemma 7], which is a trivial extension of [2, Lemma 1]. Although Bovey only states this lemma in [2] for $p = 2$, his proof applies to any prime p without change.

LEMMA 9. *Suppose that F is a form as in (1). Let p be a prime and define γ as in (4). Suppose that the system of inequalities*

$$m_0 + \cdots + m_{j-1} \geq p^j, \quad 1 \leq j \leq \gamma,$$

holds. Then the congruence $F \equiv 0 \pmod{p^\gamma}$ has a solution $\mathbf{x} = (x_1, \ldots, x_s)$ such that, for some j, neither a_j nor x_j is divisible by p.

Our final lemma is [6, Lemma 1]. This lemma is attributed to Schur [11], although the proof given in [6] is particularly simple.

LEMMA 10. *Suppose that $f(x)$ is a nonconstant polynomial. Then there are infinitely many primes p such that the congruence $f(x) \equiv 0 \pmod{p}$ has a solution.*

3. Evaluating $\Gamma^*(k)$

In this section, we begin the proofs of Theorems 2 and 3 by calculating the values of $\Gamma^*(k)$ for k given in the theorems. In the next section, we finish the proofs by showing that the required congruence conditions on $\Gamma^*(k)$ hold. In order to show that $\Gamma^*(k) = \Gamma^*(k, q)$, we first find the value of $\Gamma^*(k, q)$ and then show that if $p \neq q$ is any prime, then $\Gamma^*(k, p) \leq \Gamma^*(k, q)$.

To find the value of $\Gamma^*(k, q)$, we begin by writing $k = (\tau + 1)q + r$ with $0 \leq r \leq \tau$. Then Lemma 4 gives us

$$\Gamma^*(k, q) = (q^{\tau+1} - 1)\left(\frac{k - r}{\tau + 1}\right) + q^r.$$

Now suppose that p is a prime with $p \neq q$. In all of the lemmas that follow, our goal is to show that any additive form F as in (1) in exactly $s = \Gamma^*(k, q)$ variables must have a p-adic zero. Without loss of generality, we may assume that F has the properties in Lemma 5. We begin with a simple lemma.

LEMMA 11. *For an odd prime q and integer $\tau \geq 2$, set $k = q^\tau(q - 1)$ and $s = \Gamma^*(k, q)$. Then we have*

$$s > \frac{k^2}{\tau + 1} + q^r$$

and

$$s/k > \frac{k}{\tau + 1}.$$

Proof. Since $q \geq 3$ and $\tau \geq 2$, we have $q^\tau \geq 2r + 1$. Hence we have

$$\begin{aligned}
(q^{\tau+1} - 1)\left(\frac{k - r}{\tau + 1}\right) + q^r &\geq (q^{\tau+1} - q^\tau + 2r)\left(\frac{k - r}{\tau + 1}\right) + q^r \\
&= (k + 2r)\left(\frac{k - r}{\tau + 1}\right) + q^r \\
&= \frac{k^2}{\tau + 1} + \frac{r}{\tau + 1}(k - 2r) + q^r \\
&> \frac{k^2}{\tau + 1} + \frac{r}{\tau + 1}(q^\tau - 2r) + q^r \\
&> \frac{k^2}{\tau + 1} + q^r.
\end{aligned}$$

This proves the first statement. The second statement is now trivial since $q^r/k > 0$. This completes the proof of the lemma. □

In our next two lemmas, we show that $\Gamma^*(k, p) \leq \Gamma^*(k, q)$ for the primes p dividing k.

LEMMA 12. *Let $q \geq 3$ be a prime, let $\tau \geq 2$, and write $k = q^\tau(q - 1)$. Suppose that $p \neq q$ is an odd prime, and that $p|k$. Then we have $\Gamma^*(k, p) \leq \Gamma^*(k, q)$.*

Proof. Since $p \neq q$ and $p|k$, we must have $p|(q-1)$. Write $q-1 = p^\sigma k_0$, where $p \nmid k_0$. We need to show that if F is an additive form of degree k in $s = \Gamma^*(k,q)$ variables, then F has a nontrivial p-adic zero. By Lemma 9, we need to show that the inequality

$$v_0 + v_1 + \cdots + v_{j-1} \geq p^j \tag{6}$$

holds for each j with $1 \leq j \leq \sigma + 1$.

Now, by Lemma 5 and Lemma 11, for each j under consideration, we have

$$\begin{aligned} v_0 + \cdots + v_{j-1} &\geq js/k \\ &> jk/(\tau+1) \\ &= jq^\tau p^\sigma k_0/(\tau+1) \\ &\geq p^\sigma \left(\frac{q^\tau}{\tau+1} \right) \\ &> p^\sigma \left(\frac{p^\tau}{\tau+1} \right). \end{aligned}$$

We claim that $p^\tau/(\tau+1) \geq p$ for any p, τ under consideration. Assuming for the moment that this is true, we now have

$$v_0 + \cdots + v_{j-1} > p^{\sigma+1} \geq p^j$$

for $0 \leq j \leq \sigma + 1$, as desired.

To prove the claim, let $f(p,\tau) = p^\tau/(\tau+1) - p$, and note that if $p \geq 3$ and $\tau \geq 2$, then f is increasing in each variable. Then, for any p, τ under consideration, we have

$$\frac{p^\tau}{\tau+1} - p = f(p,\tau) \geq f(3,2) = \frac{3^2}{3} - 3 = 0.$$

Hence $p^\tau/(\tau+1) \geq p$, as desired. This completes the proof of the lemma. □

LEMMA 13. *Let $q \geq 5$ be a prime, let $\tau \geq 2$, and write $k = q^\tau(q-1)$. Then we have $\Gamma^*(k,2) \leq \Gamma^*(k,q)$.*

Proof. We prove this in essentially the same way as Lemma 12. The main difference is that we need to satisfy one extra inequality in order to use Lemma 9. As before, write $q - 1 = 2^\sigma k_0$ with k_0 odd. We now need to have

$$v_0 + \cdots + v_{j-1} \geq 2^j \quad \text{for } 1 \leq j \leq \sigma + 2.$$

By Lemma 5 and Lemma 11, we have

$$\begin{aligned} v_0 + \cdots + v_{j-1} &\geq js/k \\ &> jk/(\tau+1) \\ &= jq^\tau 2^\sigma k_0/(\tau+1) \\ &\geq 2^\sigma \left(\frac{q^\tau}{\tau+1} \right). \end{aligned}$$

As in the proof of Lemma 12, the function $f(q,\tau) = q^\tau/(\tau+1)$ is increasing in both variables. Therefore, for any q, τ under consideration, we have

$$\frac{q^\tau}{\tau+1} \geq \frac{5^2}{2+1} > 8.$$

Thus we have

$$\begin{aligned} v_0 + \cdots + v_{j-1} &> 2^\sigma \left(\frac{q^\tau}{\tau+1} \right) \\ &> 2^\sigma \cdot 8 \\ &> 2^{\sigma+2}. \end{aligned}$$

Hence each of the inequalities is satisfied. This completes the proof of the lemma. □

Now that we have dealt with the primes dividing k, we turn to the primes p that do not divide k. Our first goal is to treat the primes for which $(k, p-1) < k$, where $(*,*)$ represents the greatest common divisor. We do this in the following lemma.

LEMMA 14. *Let $\tau \geq 2$ be an integer. Suppose that $q \geq 3$ is a prime satisfying Condition $C(\tau)$ or Condition $D(\tau)$. Let p be a prime with $p \nmid k$, and define $d = (k, p-1)$. If $d \neq k$, then $\Gamma^*(k,p) \leq \Gamma^*(k,q)$.*

Proof. Suppose that $F(\mathbf{x})$ is an additive form as in (1) of degree k in $s = \Gamma^*(k,q)$ variables. Without loss of generality, we may suppose that F has the properties given in Lemma 5. Since $p \nmid k$, Hensel's lemma tells us that it suffices to show that the congruence

$$F(\mathbf{x}) \equiv 0 \pmod{p} \tag{7}$$

has a nontrivial solution using only the variables in F_0. Suppose that these variables are $x_1, \ldots, x_{v_0}$. We seek a nontrivial solution of the congruence

$$a_1 x_1^k + \cdots + a_{v_0} x_{v_0}^k \equiv 0 \pmod{p}.$$

Since the sets of kth powers and dth powers modulo p are the same, this is equivalent to solving the congruence

$$a_1 x_1^d + \cdots + a_{v_0} x_{v_0}^d \equiv 0 \pmod{p}. \tag{8}$$

Write $d = k/t$, where t is an integer. By hypothesis, we have $t > 1$. We now divide the proof into three cases.

Case 1: $t \geq \tau + 1$. In this case, we have

$$d \leq \frac{k}{\tau+1} < s/k \leq v_0$$

by Lemma 5 and Lemma 11. Since $d < v_0$, congruence (8) has a nontrivial solution by Chevalley's theorem. This completes the proof in this case.

Case 2: $3 \leq t \leq \tau$. Suppose first that t is divisible by an odd prime p_i. Then, since $t \neq \tau + 1$, the congruence conditions on q guarantee that $q \equiv 2 \pmod{p_i}$, and hence we have

$$k \equiv 2^\tau \not\equiv 0 \pmod{p_i}.$$

Since k is not divisible by p_i, it is also not divisible by t, and hence $d = k/t$ is impossible.

If t is not divisible by any odd prime, then $t \geq 4$ is a power of 2. In this case, since $q \equiv 3 \pmod 4$, we have

$$k \equiv 3^\tau \cdot 2 \equiv 2 \not\equiv 0 \pmod 4.$$

Since k is not divisible by 4, it is again not divisible by t, and $d = k/t$ is impossible. Therefore this case of the lemma cannot occur.

Case 3: $t = 2$. In this case, we have $d = k/2$. Now, since $q \equiv 3 \pmod 4$, we have as above that $k \equiv 2 \pmod 4$, and hence $d = k/2$ is odd. However, k and $p-1$ are both even, and so $d = (k, p-1)$ should be even, which is a contradiction. Hence this case also cannot occur. This completes the proof of the lemma. □

Finally, we deal with the primes for which $(k, p-1) = k$. We begin with the following preliminary lemma.

LEMMA 15. *Suppose that τ is not divisible by 4. If q is a prime satisfying either Condition C(τ) or Condition D(τ), then $k+1$ is composite. If τ is divisible by 4, then there exist infinitely many primes satisfying Condition C(τ) such that $k+1$ is composite, and there also exist infinitely many primes satisfying Condition D(τ) such that $k+1$ is composite.*

Proof. If τ is odd, then the condition that $q \equiv 2 \pmod 3$ gives us

$$k + 1 \equiv 2^\tau (2-1) + 1 \equiv 0 \pmod 3.$$

Since $k + 1 > 3$, this number is composite.

If τ is even but not divisible by 4, then since $q \equiv 2 \pmod 5$, we have

$$k + 1 \equiv 2^\tau (2-1) + 1 \equiv 2^2 + 1 \equiv 0 \pmod 5.$$

Since $k + 1 > 5$, this number is composite.

Finally, suppose that τ is divisible by 4. Select a prime $P > \tau + 1$ and a number C such that $C^\tau (C-1) + 1 \equiv 0 \pmod P$. This is possible by Lemma 10. Note that $C \not\equiv 0 \pmod P$. Now, consider the system of congruences in either Condition C(τ) or Condition D(τ), along with the additional congruence $q \equiv C \pmod P$. This system is equivalent to a single congruence of the form

$$q \equiv A \pmod{60 p_1 \cdots p_t P},$$

where A is relatively prime to $60 p_1 \cdots p_t P$. By Dirichlet's theorem, there exist infinitely many primes satisfying this congruence. If the prime q satisfies the congruence and is sufficiently large, then q satisfies Condition C(τ) (or Condition D(τ), as desired). Also, $k+1$ is composite, as it is divisible by P. This completes the proof of the lemma. □

LEMMA 16. *Suppose that a prime q satisfies either Condition C(τ) or Condition D(τ). If τ is divisible by 4, then assume additionally that $k+1$ is composite. Then we have $\Gamma^*(k) = \Gamma^*(k, q)$.*

Proof. By the previous lemmas, we know that $\Gamma^*(k, p) \leq \Gamma^*(k, q)$ for all primes p except possibly for those for which $(k, p-1) = k$. We are finished if we can show that the inequality holds for these remaining primes, so let p be one of them. By either Lemma 15 (for $4 \nmid \tau$) or hypothesis (for $4|\tau$), we know that $k+1$ is composite. Therefore we have $1 < k < p-1$.

As before, suppose that $F(\mathbf{x})$ is defined as in (1), with $s = \Gamma^*(k, q)$, and satisfies the properties in Lemma 5, so that we have $v_0 > k/(\tau+1)$. Then we have

$$v_0 \geq s/k > k/(\tau+1) > 12k^{7/8}(\log k)^2.$$

Therefore Lemma 8 implies that F has nontrivial p-adic zeros. This completes the proof of the lemma. □

4. Congruences for $\Gamma^*(k)$

In this section, we finish the proofs of Theorems 2 and 3. After the results of Section 3, we know that $\Gamma^*(k) = \Gamma^*(k, q)$ for all values of k in the theorems. Hence we simply need to determine whether $\Gamma^*(k, q) \equiv 1 \pmod{k}$. We begin with a lemma which tells us exactly when this congruence holds for our values of k.

LEMMA 17. *Suppose that a prime q satisfies either Condition $C(\tau)$ or Condition $D(\tau)$, and if τ is divisible by 4, assume additionally that $k+1 = q^\tau(q-1)+1$ is composite. Then we have $\Gamma^*(k) \equiv 1 \pmod{k}$ if and only if $(\tau+1)|(q-1)$.*

Proof. Let r, with $0 \leq r < \tau+1$, be the remainder when k is divided by $\tau+1$, and note that since $q > \tau+1$, we have $r = 0$ if and only if $(\tau+1)|(q-1)$. Then Lemma 4 gives us

$$\Gamma^*(k) = \Gamma^*(k, q) = (q^{\tau+1}-1)\left(\frac{k-r}{\tau+1}\right) + q^r.$$

Suppose first that $r = 0$, so that $\tau+1$ divides $q-1$. Then we have

$$\begin{aligned}\Gamma^*(k, q) &= (q^{\tau+1}-1)\left(\frac{k}{\tau+1}\right) + 1 \\ &= (q-1)(q^\tau + q^{\tau-1} + \cdots + 1)\left(\frac{k}{\tau+1}\right) + 1 \\ &= \left(\frac{q-1}{\tau+1}\right)(q^\tau + q^{\tau-1} + \cdots + 1)k + 1 \\ &\equiv 1 \pmod{k}.\end{aligned}$$

Suppose instead that $r \neq 0$, so that $(\tau+1) \nmid (q-1)$. Then we have

$$\Gamma^*(k, q) \equiv (-1)\left(\frac{k-r}{\tau+1}\right) \pmod{q}.$$

We claim that the fraction in parentheses is not congruent to -1 modulo q. To see this, suppose that it were congruent to -1. Then we would obtain

$$k - r \equiv (\tau+1)(-1) \pmod{q},$$

where, since $q > \tau + 1$, we are not merely multiplying both sides of the congruence by zero. This would give us

$$r \equiv \tau + 1 \pmod{q}.$$

But since r and $\tau + 1$ are both positive and smaller than q, we would have $r = \tau + 1$, a contradiction. Therefore $\Gamma^*(k, q) \not\equiv 1 \pmod{q}$. Since $q|k$, we also have $\Gamma^*(k, q) \not\equiv 1 \pmod{k}$. This completes the proof of the lemma. □

We can now easily complete the proofs of Theorems 2 and 3. In order to prove Theorem 3, suppose that q is a prime satisfying the hypotheses of the theorem. Then, by either Lemma 15 (if $4 \nmid \tau$) or hypothesis (if $4|\tau$), we know that $k + 1$ is composite. For these primes, we have $q \equiv 1 \pmod{\tau + 1}$, which immediately implies that $(\tau + 1)|(q - 1)$. Lemma 17 now finishes the proof.

To prove Theorem 2, suppose that q is a prime satisfying Condition C(τ). If τ is divisible by 4, then suppose further that $k + 1$ is composite. We know that $\Gamma^*(k) = \Gamma^*(k, q)$. Now, suppose that $\tau + 1$ is divisible by an odd prime p_i. Then from Condition C(τ) we know that $q \equiv 2 \pmod{p_i}$. Then $q - 1$ is not divisible by p_i, and hence not divisible by $\tau + 1$. Otherwise, we know that $\tau + 1 \geq 4$ is a power of 2. In this case, the condition that $q \equiv 3 \pmod 4$ shows us that $q - 1$ is not divisible by 4, and hence again not divisible by $\tau + 1$. Then Lemma 17 again finishes the proof.

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. Chevalley, *Démonstration d'une hypothèse de M. Artin,* Abh. Math. Semin. Univ. Hambg. 11 (1935), 73–75.

[4] H. Davenport and D. J. Lewis, *Homogeneous additive equations,* Proc. R. Soc. Lond. Ser. A 274 (1963), 443–460.

[5] M. Dodson, *Homogeneous additive congruences,* Philos. Trans. R. Soc. Lond. Ser. A 261 (1967), 163–210.

[6] I. Gerst and J. Brillhart, *On the prime divisors of polynomials,* Amer. Math. Monthly 78 (1971), 250–266.

[7] H. Godinho, M. Knapp, P. H. A. Rodrigues, and D. Veras, *On the values of* $\Gamma^*(k, p)$ *and* $\Gamma^*(k)$, Acta Arith. 191 (2019), 67–80.

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

[9] ———, *2-Adic zeros of diagonal forms,* J. Number Theory 193 (2018), 37–47.

[10] K. K. Norton, *On homogeneous diagonal congruences of odd degree,* Ph.D. thesis, University of Illinois, 1966.

[11] I. Schur, *Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen,* Sitzungsber. Berl. Math. Ges. 11 (1912), 40–50.

[12] I. M. Vinogradov, *The method of trigonometrical sums in the theory of numbers,* Interscience Publishers, London, and New York. Translated, revised and annotated by K. F. Roth and Anne Davenport.

H. Godinho
Departamento de Matemática
Universidade de Brasília
Brasília
DF 70910-900
Brazil

hemar@mat.unb.br

M. P. Knapp
Department of Mathematics and Statistics
Loyola University Maryland
4501 North Charles Street
Baltimore, MD 21210-2699
USA

mpknapp@loyola.edu