Simultaneous additive congruences of different degrees to a large prime modulus

Michael P. Knapp, Bruno de Paula Miranda, Paulo H. A. Rodrigues

Dedicated to Trevor Wooley on the occasion of his 60th birthday.

Abstract

Let p be a prime number. For positive integers $k_1 > \cdots > k_R$, define the number $\Gamma_p^*(k_1, \dots, k_R)$ to be the smallest number s of variables such that any system of equations of the form

$$a_{i1}x_1^{k_i} + \cdots + a_{is}x_s^{k_i} = 0 \qquad (1 \leq i \leq R)$$

with coefficients in the p-adic field $\mathbb{Q}_p$ has a nontrivial solution. In this article, we find upper bounds for $\Gamma_p^*(k_1, \dots, k_R)$ under the assumption that $p > k_1^4$. In particular, we show that under this condition, we have $\Gamma_p^*(k_1, k_2) \leq 2k_1 + 6k_2 + 1$ and $\Gamma_p^*(k_1, k_2, k_3) \leq 2k_1 + 14k_2 + 15k_3 + 1$. We also prove a general bound that applies for any number of equations.

1 Introduction

In this article, we study p-adic zeros of a system of diagonal polynomials of different degrees when p is large compared to those degrees. Specifically, consider the system

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

where $k_1 > \cdots > k_R$ and the coefficients are integers of a p-adic field $\mathbb{Q}_p$. We examine the p-adic solubility of this system when p is a prime such that

$p > k_1^4$. It is well-known that, given the prime p and the degrees of the polynomials, there is a number $\Gamma_p^*(k_1, \ldots, k_R)$ such that if the number s of variables is at least $\Gamma_p^*(k_1, \ldots, k_R)$, then the system must have nontrivial p-adic solutions, regardless of the coefficients. This is true even when some or all of the polynomials have the same degrees. In fact, it is even known that if we define

$$\Gamma^*(k_1, \ldots, k_R) = \max_{p \text{ prime}} \Gamma_p^*(k_1, \ldots, k_R),$$

then $\Gamma^*(k_1, \ldots, k_R)$ is defined for all sets of degrees. Therefore, given the degrees, there is a single number of variables that will suffice to guarantee solubility for all primes.

A conjecture commonly attributed to Emil Artin (see the introduction to [3]) states that for any degrees $k_1, \ldots, k_R$, we should have $\Gamma^*(k_1, \ldots, k_R) \leq k_1^2 + \cdots + k_R^2 + 1$. For a single polynomial, this was proved by Davenport & Lewis [5] in the first paper of their pioneering work on Artin's conjecture. For larger systems, most work has focused on the case where the degrees of the polynomials are all equal. In this setting, Knapp [10] has shown that $\Gamma^*(k, k, \ldots, k) \leq 4R^2k^2$, where R is the number of equations. This is currently the best bound that holds for all values of R and k. When the degrees are different, Artin's conjecture is known to fail (see any of [1, 4, 14], which were published independently and at about the same time), even for systems of only two polynomials (see [19]). In this case, the best known result that holds for any set of degrees is the bound

$$\Gamma^*(k_1, \ldots, k_R) \leq (k_1^2 + 1) \cdots (k_R^2 + 1)$$

due to Leep & Schmidt, which follows trivially from [13, Equation (2.11)].

It transpires that the worst obstructions to solving (1) occur at relatively small primes, and that if the prime p is assumed to be large, then significantly fewer variables are required to guarantee solubility. For a single equation, Dodson [6, Lemma 2.4.1] has shown that if $p > k^4$, then $\Gamma_p^*(k) \leq 2k + 1$. Again, the majority of work on systems for large primes has focused on the situation where the polynomials all have the same degree. In this direction, Meir [16] has shown that $\Gamma_p^*(k, k) \leq 4k + 1$ whenever $p > 3k^4$, and Atkinson, Brüdern, & Cook [2] have shown that for any number R of equations, we have $\Gamma_p^*(k, k, \ldots, k) \leq 2Rk + 1$ whenever $p > k^{2R+2}$. All of these results are best possible in the sense that the upper bound on the number of variables cannot be reduced. In a somewhat different direction, Godinho & Rodrigues [8] have shown that if p satisfies the condition that every congruence of the form $a_1x_1^k + a_2x_2^k + a_3x_3^k \equiv b \pmod{p}$ with $a_1a_2a_3 \not\equiv 0 \pmod{p}$ has a solution with $x_1x_2x_3 \not\equiv 0 \pmod{p}$, then we have $\Gamma^*(k, k, \ldots, k) \leq 2 \cdot 3^{R-1} \cdot k + 1$. While this upper bound is worse than the others discussed, the condition on p may well be satisfied for primes smaller than are allowed in these other results.

For systems of equations of different degrees, little is known. Wooley [18] has shown that $\Gamma_p^*(k_1, k_2) \leq 2(k_1 + k_2) + 1$ whenever $p > k_1^4k_2^2$ (recall that $k_1 > k_2$), with better bounds when $k_2 = 1$. Like the results for equal degrees above, Wooley's result is best possible in the sense that the upper bound cannot be reduced. Moreover, he conjectured in [18] that we have $\Gamma_p^*(k_1, \ldots, k_R) \leq 2(k_1 + \cdots + k_R) + 1$ whenever $p > k_1^4(k_2 \cdots k_R)^2$, again with a slightly modified bound when $k_R = 1$. Knapp [11] has shown that if $p > k_1 - k_R + 1$, then we have

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

While this is a much worse upper bound, it applies even for some primes smaller than the largest degree in the system. Knapp has also [12] given a bound for $\Gamma_p^*(k_1, \ldots, k_R)$ in the situation where some of the polynomials may have the same degree, while others have different degrees.

In this article, we prove some results about equations of different degrees which fall somewhere between those of Wooley and Knapp mentioned above. While we see that our bounds are worse than those of Wooley, we only assume in our results that $p > k_1^4$. We note that unlike Knapp's bound mentioned above, our current bounds are linear in the degrees of the polynomials. Our first two results give bounds for $R = 2$ and $R = 3$ equations.

Theorem 1. *Suppose that k, n are positive integers with $k > n$. If $p > k^4$, then we have*

$$\Gamma_p^*(k, n) \leq 2k + 6n + 1.$$

Theorem 2. *Suppose that k_1, k_2, k_3 are positive integers with $k_1 > k_2 > k_3$. If $p > k_1^4$, then we have*

$$\Gamma_p^*(k_1, k_2, k_3) \leq 2k_1 + 14k_2 + 15k_3 + 1.$$

Our final theorem gives a general bound that holds for any number $R \geq 4$ of equations.

Theorem 3. *Suppose that $k_1, k_2, \ldots, k_R$ are positive integers with $k_1 > k_2 > \cdots > k_R$. If $p > k_1^4$, then we have*

$$\begin{aligned}\Gamma_p^*(k_1, k_2, \ldots, k_R) \leq \sum_{i=1}^{R-3} \left(i \cdot 3^{R-3} - 1\right) k_i + \left((R+1) \cdot 3^{R-3} - 1\right) k_{R-2} \\ + \left((R+14) \cdot 3^{R-3} - 1\right) k_{R-1} + \left((R+30) \cdot 3^{R-3} - 1\right) k_R + 1.\end{aligned}$$

We note that the bound in Theorem 3 is of lower quality than the bounds in Theorem 1 and Theorem 2. In our first two theorems, we work to prove the best bound that we can, while for the final theorem we prioritize finding a relatively simple argument that can be used regardless of the number of equations in the system.

As with most theorems about solving p-adic equations, the main goal in our proofs is to find a nonsingular solution of a system of associated congruences, which then lifts to a solution of the p-adic system by Hensel's lemma. The primary methods we use to solve the congruences are contractions and exponential sums. Contractions, which will be more fully explained in Section 2, essentially allow us to combine several variables into a single new variable in a way that yields desirable properties. For example, if we are able to use the variables x_1, x_2, x_3 to solve the congruence of degree k_1, then we can "contract" them into a new variable T whose coefficient in the degree k_1 congruence is 0. Thus, any value of T yields a solution of the degree k_1 congruence when traced back to the x-variables. Exponential sums are also a common tool used in solving congruences, especially for large primes. They have been used to prove good results about the number of solutions of congruences, and we make great use of these results in our proofs.

This article is structured as follows. In Section 2 and Section 3, we give the preliminary lemmas that we will use in the proofs of the theorems.

Section 2 contains preliminary lemmas of a more elementary nature, while Section 3 contains the lemmas which stem from exponential sums. Then Section 4, Section 5, and Section 6 give the proofs of Theorem 1, Theorem 2, and Theorem 3, respectively.

2 Basic Preliminaries

In this section and the next, we give the preliminary lemmas that are needed in the proofs of the theorems. In this section, we give the lemmas which we either quote from other sources or can prove without techniques involving either algebraic geometry or exponential sums.

Throughout this article, p is considered to be a fixed prime with $p > k_1^4$. The majority of our work will involve solving congruences modulo p. Therefore, we will always consider variables and coefficients modulo p. So for example, if we say that a variable x has a nonzero coefficient, we really mean that it is nonzero modulo p unless we explicitly state otherwise.

If x_i is a variable in the system (1), then we will call the vector $\begin{pmatrix} a_{1i} \\ \vdots \\ a_{Ri} \end{pmatrix}$ the *coefficient vector* of x_i. When dealing with coefficient vectors, we will typically only be concerned with whether or not a given coefficient is zero modulo p. To make this clear, we will use an asterisk $(*)$ to represent a number that is nonzero modulo p and a dash $(-)$ to represent a number for which we do not know whether it is zero modulo p. So for example, if we say that x_1 has the coefficient vector $\begin{pmatrix} 0 \\ * \\ - \end{pmatrix}$, this means that x_1 has a zero (modulo p) coefficient in the degree k_1 polynomial, a nonzero (modulo p) coefficient in the degree k_2 polynomial, and we do not know whether or not the coefficient of x_1 in the degree k_3 polynomial is zero modulo p.

Our first lemma states that it is sufficient to consider only systems whose coefficients have certain desirable properties when considered modulo p.

Lemma 4. *Consider the system* (1)*, where the equations all have different degrees $k_1, \ldots, k_R$. We may assume that* (1) *is normalized as defined in [11], in the sense that if all normalized systems have nontrivial solutions, then so* *do all non-normalized systems. Suppose that the polynomials in a normalized system are written in the form*

$$F_i = f_i(x_1, \ldots, x_N) + pg_i(x_{N+1}, \ldots, x_s)$$

for $i = 1, \ldots, R$, where $x_1, \ldots, x_N$ are the variables which appear in at least one equation with a coefficient not divisible by p. Let r be a number with $R \le r \le s$, and for fixed numbers $m_1, \ldots, m_{R-1}$ with $r+1 \le m_1 \le \cdots \le m_{R-1} \le s$, define

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

Then the following statements are true.

1. *If N is the number of variables in* (1) *which are explicit when* (1) *is reduced modulo p, then one has*

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

2. *If q_i is the number of variables explicit in the form F_i of degree k_i after reducing modulo p, then one has*

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

3. *If q_{ij} is the total number of variables which are explicit in either the form F_i of degree k_i or the form F_j of degree k_j after reducing modulo p, then one has*

$$q_{ij} \ge \left(|M_i| + \frac{r}{R}\right) \frac{1}{k_i} + \left(|M_j| + \frac{r}{R}\right) \frac{1}{k_j}.$$

Proof. The fact that we may assume that (1) is p-normalized is stated in [11] and is a commonly used fact when proving theorems of this type. The first two numbered statements are the content of [11, Lemma 4].

The third statement is new. To prove it, we use the notation developed in [11] without explicitly defining it here. Suppose without loss of generality that the variables in the polynomials F_i and F_j which are explicit modulo p are $x_1, \ldots, x_{q_{ij}}$, and consider the new system

$$\mathbf{F}' = \mathbf{bF}(px_1, \ldots, px_{q_{ij}}, x_{q_{ij}+1}, \ldots, x_s),$$

where $\mathbf{b} = (b_1, \ldots, b_R)$ with $b_i = b_j = p^{-1}$ and $b_\ell = 1$ otherwise. Again using the notation from [11], we have $\partial(\mathbf{F}') = p^B \partial(\mathbf{F})$, where

$$B = \frac{RLKq_{ij}}{r} - \left(L + \frac{|M_i|RL}{r}\right) k_i' - \left(L + \frac{|M_j|RL}{r}\right) k_j'.$$

Since the system (1) is assumed to be normalized, the normalization process guarantees that $B \geq 0$. Recalling from [11] that $k_i' = K/k_i$ and $k_j' = K/k_j$, the third part of the lemma follows. This completes the proof. □

In the proofs of Theorem 2 and Theorem 3, we will need a slightly generalized definition of the values q_i and q_{ij} given in Lemma 4. If S is any set of variables, then we define $q_i(S)$ to be the number of variables in S which have a nonzero coefficient in the congruence of degree k_i, and define $q_{ij}(S)$ to be the number of variables in S which have a nonzero coefficient in either the degree k_i congruence or the degree k_j congruence. The values q_i and q_{ij} in Lemma 4 can be thought of as $q_i(S)$ and $q_{ij}(S)$, where either $S = \{x_1, \ldots, x_s\}$ or $S = \{x_1, \ldots, x_N\}$.

Once we have a normalized system, the goal in our proofs will be to solve the system modulo p and then lift that solution of congruences to a p-adic solution. We do this through the version of Hensel's lemma below. This is not the most general version possible, but it suffices for our purposes since none of the degrees of the equations will be divisible by p. A good exposition of Hensel's lemma can be found in [9]

Lemma 5. *Consider the system* (1), *and suppose that when this system is reduced modulo p, the resulting system of congruences is*

$$\begin{array}{rcl} a_{11}x_1^{k_1} + \cdots + a_{1N}x_N^{k_1} & \equiv & 0 \pmod{p} \\ \vdots & & \vdots \\ a_{R1}x_1^{k_R} + \cdots + a_{RN}x_N^{k_R} & \equiv & 0 \pmod{p}, \end{array} \qquad (2)$$

where each of the variables $x_1, \ldots, x_N$ appears in at least one of the congruences with a nonzero (modulo p) coefficient. Suppose that $(\epsilon_1, \ldots, \epsilon_N)$ is a solution of this system, and let J be the Jacobian matrix $(\partial F_i/\partial x_j)(\epsilon_1, \ldots, \epsilon_N)$. If J has rank R, then the solution $(\epsilon_1, \ldots, \epsilon_N)$ of (2) *lifts to a nontrivial solution of* (1) *in $\mathbb{Q}_p^s$.*

One main tool that we will use in our proofs is the idea of making a contraction of variables. This is simply the idea of setting some variables equal to multiples of others in a way that creates nice properties. Suppose that we have a collection of variables, for example $x_1, \ldots, x_R$, with coefficients $a_1, \ldots, a_R$ in an equation of degree k. Suppose further that $t_1, \ldots, t_R$ are integers of $\mathbb{Q}_p$ such that $a_1 t_1^k + \cdots + a_R t_R^k = b$. We may then contract these variables to a single new variable T by setting $x_i = t_i T$ for $i = 1, \ldots, R$. This new variable will then have coefficient b in this equation. In our proofs, the main power of contractions will be to allow us to guarantee that certain nontrivial solutions are in fact nonsingular. For example, suppose that in the system of congruences (2), we can set $(x_1, \ldots, x_R) = (t_1, \ldots, t_R)$ in such a way that the first R columns of the Jacobian J have rank R. If we then set $x_i = t_i T$ $(i = 1, \ldots, R)$, we obtain a new system of congruences. If we can solve this new system with $T \not\equiv 0 \pmod{p}$, then when we trace this solution back to the original x-variables, the Jacobian will have rank R and we will be able to use Hensel's lemma to find a p-adic solution. The following lemma [11, Lemma 10] allows us to guarantee in many cases that it is possible to find $t_1, \ldots, t_R$ with this property.

Lemma 6. *Consider the matrix*

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

and assume that $a_{11}a_{22}\cdots a_{RR} \not\equiv 0 \pmod{p}$. If $p > k_1 - k_R + 1$, then there exist integers $t_2, \ldots, t_R$, all relatively prime to p, such that if we set $x_j = t_j x_1$ for $2 \le j \le R$ and let x_1 be any integer relatively prime to p, then $\det B \not\equiv 0 \pmod{p}$.

Proof. This lemma is proven in [11]. We repeat the proof here because in order to prove Corollary 7 below, we need information from the proof rather than just the statement of the Lemma.

First note that if we set $x_2 = t_2x_1, \dots, x_R = t_Rx_1$, then we have

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

where C is the matrix

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

Since we require $x_1, t_2, \dots, t_R$ to all be nonzero modulo p, we have $\det B \not\equiv 0 \pmod{p}$ if and only if $\det C \not\equiv 0 \pmod{p}$.

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

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

and the matrix C becomes

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

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

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

and by expanding along the rightmost column we get

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

where

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

is a polynomial with no constant term. If $c_1, \ldots, c_{M-1}$ are all divisible by p, then any value of t_M yields

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

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

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

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

In this proof, note that the acceptable values of t_M are exactly the values that make a particular polynomial nonzero, and that this polynomial has degree at most $k_1 - k_M$. Therefore, this polynomial has at most $k_1 - k_M$ zeros, and there are at least $(p-1) - (k_1 - k_M)$ values of t_M that make the polynomial nonzero. Then we clearly have the following corollary. The second statement in the corollary follows from the fact that we may set x_1 to be any nonzero value.

Corollary 7. *In Lemma 6, there are at least*

$$\prod_{i=2}^{R} \Big((p-1) - (k_1 - k_i) \Big)$$

ways to choose the numbers $t_2, \ldots, t_R$. Hence there are

$$(p-1) \prod_{i=2}^{R} \Big((p-1) - (k_1 - k_i) \Big)$$

R-tuples $(x_1, \ldots, x_R)$ that lead to a new variable T with the nonsingularity property discussed before the statement of Lemma 6.

Our final two results in this section provide a bound on how many variables are required to solve certain systems of congruences. Our first lemma is essentially [16, Lemma 8].

Lemma 8. *Suppose that $p > k^4$. If $a_1a_2a_3 \not\equiv 0 \pmod{p}$, then the congruence*

$$a_1x_1^k + a_2x_2^k + a_3x_3^k \equiv b \pmod{p}$$

has a solution with $x_1x_2x_3 \not\equiv 0 \pmod{p}$.

In [16], Meir adds the condition that $p \equiv 1 \pmod{k}$, but it is easy to see that this is not needed. If $p \not\equiv 1 \pmod{k}$, let $d = \gcd(k, p-1)$. Then we have $p > d^4$ and $p \equiv 1 \pmod{d}$. Thus the lemma holds for an equation of degree d. However, the set of d-th powers modulo p is identical to the set of k-th powers modulo p, and so the lemma must also hold for degree k.

Our last lemma in this section allows us to solve systems of congruences. We will use this in the proof of Theorem 3. The idea of the proof has been used a number of times before, for example in the proof of the Leep-Schmidt bound for $\Gamma^*(k_1, \ldots, k_R)$ mentioned in the introduction.

Lemma 9. *Suppose that $k_1 \geq \cdots \geq k_R$ are positive integers and that $p > k_1^4$. Then the system*

$$\begin{array}{rcrl} a_{11}x_1^{k_1} + \cdots + a_{1N}x_N^{k_1} & \equiv & 0 & \pmod{p} \\ \vdots & & & \vdots \\ a_{R1}x_1^{k_R} + \cdots + a_{RN}x_N^{k_R} & \equiv & 0 & \pmod{p} \end{array} \qquad (3)$$

has a nontrivial solution whenever $N \geq 3^R$.

Proof. We proceed by induction on R. If $R = 1$ then we are done by Lemma 8. Suppose now that the lemma is true when the number of equations in the system is $R-1$. If we actually have $N > 3^R$ then set $x_i = 0$ for all $i > 3^R$. Now, for $j = 0, 1, \ldots, 3^{R-1}-1$, consider the set of variables $\{x_{3j+1}, x_{3j+2}, x_{3j+3}\}$. For each set, we can nontrivially solve the congruence

$$a_{R,3j+1}x_{3j+1}^{k_R} + a_{R,3j+2}x_{3j+2}^{k_R} + a_{R,3j+3}x_{3j+3}^{k_R} \equiv 0 \pmod{p}.$$

If the solution we have found is $(\epsilon_{3j+1}, \epsilon_{3j+2}, \epsilon_{3j+3})$, then we contract these variables and set $x_{3j+i} = \epsilon_{3j+i}T_j$ for each $i \in \{1, 2, 3\}$. This results in a system of $R-1$ congruences in the variables $T_0, \ldots, T_{3^{R-1}-1}$ with the property that any nontrivial solution of this new system yields a nontrivial solution of (3) when traced back to the x-variables. Since this system has 3^{R-1} variables, the inductive hypothesis implies that it does have a nontrivial solution, completing the proof. □

Remark 10. We note that in the proof of Lemma 9, the condition that $p > k_1^4$ was only used to guarantee that for each degree k_i, any congruence of the form $a_1x_1^{k_i} + a_2x_2^{k_i} + a_3x_3^{k_i} \equiv 0 \pmod{p}$ has a nontrivial solution. It may well be possible (depending on the values of the k_i) that this congruence condition holds for smaller primes.

3 More Preliminaries

In this section, we prove more preliminary lemmas, which are related in that the proofs all come from either algebraic geometry or the theory of exponential sums. Our first lemma in this section is certainly well-known, but we have not seen a proof in the literature, although we have found proofs of nearly identical theorems on the internet (see for example the answers to [7]).

Lemma 11. *Let p be a prime and f be a polynomial $f = a_1x_1^k + a_2x_2^k + a_3x_3^k$, where $p \nmid k$ and $p \nmid a_1a_2a_3$. Then f is absolutely irreducible over $\mathbb{F}_p$. That is, f is irreducible in any algebraic extension of $\mathbb{F}_p$.*

Proof. It is enough to consider f over the field $\overline{\mathbb{F}_p}$, the algebraic closure of $\mathbb{F}_p$. In this field, since the equation $f = 0$ defines a projective curve, if f is reducible, then the partial derivatives have a common projective zero. However, for each i, we have $\frac{\partial f}{\partial x_i} = ka_ix_i^{k-1}$. Since $p \nmid ka_i$, the only way to have $\frac{\partial f}{\partial x_i} = 0$ is if $x_i = 0$. So the only common zero of the partial derivatives is $(0, 0, 0)$, but this is not a projective point. □

For the rest of the proofs in this section we will need the following lemma about the number of zeros of a single additive form modulo p. The statement of this lemma is [15, Theorem 6.36], specialized to the situation where the congruence is homogeneous. The formula for $M(d)$ is equation (6.12) of [15], and appears shortly after Theorem 6.36.

Lemma 12. *The number Z of solutions of the diagonal equation $a_1x_1^k + \cdots + a_sx_s^k \equiv 0 \pmod{p}$ satisfies*

$$|Z - p^{s-1}| \leq M(d)(p-1)p^{(s-2)/2},$$

where $d = \gcd(k, p-1)$ and $M(d)$ is given by the formula

$$M(d) = (-1)^s + \sum_{r=1}^{s}(-1)^{s-r} \sum_{1 \leq i_1 < i_2 < \cdots < i_r \leq s} d^{r-1}.$$

Lemma 13. *Suppose that k and n are positive integers with $k \neq n$ and consider a system of two polynomials*

$$\begin{aligned} f_k &= a_1x_1^k + a_2x_2^k + a_3x_3^k \\ f_n &= b_1x_1^n + b_2x_2^n + b_3x_3^n. \end{aligned}$$

Assume that $p > \max\{k^4, n^4\}$ and that the coefficients b_1, b_2, b_3 are all nonzero modulo p. Further, assume that at least one of the coefficients a_1, a_2, a_3 is nonzero modulo p. Then it is possible to find values of $\beta_1, \beta_2, \beta_3$ so that $f_n(\beta_1, \beta_2, \beta_3) \equiv 0 \pmod{p}$ and $f_k(\beta_1, \beta_2, \beta_3) \not\equiv 0 \pmod{p}$.

Proof. We know from Lemma 11 that f_n is absolutely irreducible. If $n > k$, then clearly $f_n \nmid f_k$. Also, if $k > n$, then $f_n \nmid f_k$ because either f_k only involves at most two variables or else f_k involves three variables and is absolutely irreducible. Also, since f_n is absolutely irreducible, no absolutely irreducible factor of f_k can divide f_n. Consequently, f_k and f_n do not share any absolutely irreducible factors. Now, because the equations $f_k = 0$ and $f_n = 0$ both define projective curves, Bezout's theorem says that these curves intersect in at most $k \cdot n$ distinct projective points. Therefore, the number of affine points of intersection is at most $(p-1)kn+1$. Hence we will be done if we can show that the equation $f_n \equiv 0 \pmod{p}$ has more than $(p-1)kn+1$ solutions, since there must then be at least one solution of $f_n \equiv 0 \pmod{p}$ that is not a solution of both equations.

Let Z be the number of solutions of $f_n \equiv 0 \pmod{p}$. Then from Lemma 12 we know that

$$|Z - p^2| \leq (d^2 - 3d + 2)(p-1)p^{1/2} \leq (n^2 - 3n + 2)(p-1)p^{1/2},$$

where $d = \gcd(n, p-1)$. This implies that

$$Z \geq p^2 - (n^2 - 3n + 2)(p-1)p^{1/2}.$$

So we will be done if we can prove that

$$p^2 - (n^2 - 3n + 2)(p-1)p^{1/2} > (p-1)kn + 1.$$

Suppose that $m = \max\{k, n\}$. Then it suffices to prove that

$$p^2 - (m^2 - 3m + 2)(p-1)p^{1/2} > (p-1)m^2 + 1.$$

Some algebra shows that this is true if and only if

$$p^{1/2} > \frac{m^2 - 3m + 2 + \sqrt{(m^2 - 3m + 2)^2 + 4m^2 - 4}}{2}.$$

Squaring, we will be finished if we can show that

$$p > \frac{(m^2 - 3m + 2)^2 + 2m^2 - 2}{2} + \frac{(m^2 - 3m + 2)\sqrt{(m^2 - 3m + 2)^2 + 4m^2 - 4}}{2}. \quad (4)$$

However, since $m \geq 2$, we have the inequalities

$$\begin{aligned} (m^2 - 3m + 2)^2 + 2m^2 - 2 &< m^4 \\ m^2 - 3m + 2 &< m^2 \\ (m^2 - 3m + 2)^2 + 4m^2 - 4 &< m^4. \end{aligned}$$

Inserting these inequalities into the right-hand side of (4), we can see that the right-hand side of (4) is strictly less than m^4, completing the proof. □

Lemma 14. *Consider the system of polynomials*

$$\begin{aligned} a_1x_1^k + a_2x_2^k + a_3x_3^k &\equiv 0 \pmod{p} \\ b_1x_1^n + b_2x_2^n + b_3x_3^n &\equiv 0 \pmod{p}, \end{aligned} \quad (5)$$

where $k > n$ and $a_1, b_1, b_2, b_3 \not\equiv 0 \pmod{p}$. If $p > k^4$, then we can find a solution of the degree n congruence with $x_1 \not\equiv 0 \pmod{p}$ and with $x_2 = tx_1$, where t is a number satisfying the properties in Lemma 6.

Proof. To begin, we bound the number of solutions of the degree n congruence that do not have the stated property. First, suppose that $x_1 \not\equiv 0 \pmod{p}$, and note that there are $p-1$ such values. As we have seen in the proof of Lemma 6, there are at most $k-n$ values of t which do not have the required property. If we set $x_2 = tx_1$, where t is one of these bad values, then there is only one possible value of x_3^n which solves the degree n equation, and hence there are at most $\gcd(p-1,n)$ values of x_3. This gives a total of at most $(p-1)(k-n)\cdot\gcd(p-1,n)$ "bad" solutions with $x_1 \not\equiv 0 \pmod{p}$. On the other hand, if $x_1 \equiv 0 \pmod{p}$ in a solution, then either $x_2 \equiv x_3 \equiv 0 \pmod{p}$, or else $x_2 \not\equiv 0 \pmod{p}$ and there are at most $\gcd(p-1,n)$ values of x_3 which yield a solution. Hence, the number of "bad" solutions of the degree n congruence is at most

$$\begin{aligned}(p-1)(k-n)\cdot\gcd(p-1,n) + 1 + (p-1)\cdot\gcd(p-1,n)\\ = (p-1)(k-n+1)\cdot\gcd(p-1,n)+1.\end{aligned}$$

Next, let Z be the total number of solutions of the degree n congruence. By Lemma 12, we have

$$|Z - p^2| \leq (n^2-3n+2)(p-1)p^{1/2}.$$

Hence we have

$$Z \geq p^2 - (n^2-3n+2)(p-1)p^{1/2}.$$

If the right-hand side of this expression is greater than the maximum possible number of "bad" solutions, then there must be a solution with the required properties. So we are finished if we have

$$p^2 - (n^2-3n+2)(p-1)p^{1/2} \geq 1 + \left[(p-1)(k-n+1)\cdot\gcd(p-1,n)+1\right].$$

That is, we are done if we have

$$p^2 \geq (n^2-3n+2)(p-1)p^{1/2} + (p-1)(k-n+1)\cdot\gcd(p-1,n)+2.$$

If it happens that $n=1$ or $n=2$, then $n^2-3n+2=0$, and we only need to have

$$p^2 \geq (p-1)(k-n+1)\cdot\gcd(p-1,n)+2.$$

Since we have

$$\begin{aligned}(p-1)(k-n-1)\cdot \gcd(p-1,n)+2 &\leq (p-1)(k-n+1)n+2\\ &\leq (p-1)k^2+2\\ &= pk^2-k^2+2\\ &< pk^2,\end{aligned}$$

it is enough to have $p^2 \geq pk^2$, or in other words $p \geq k^2$. The hypothesis $p > k^4$ certainly suffices in this case.

Now suppose that $n \geq 3$. For these values, it suffices to show that

$$p^2-1 \geq (n^2-3n+2)(p-1)p^{1/2}+(p-1)(k-n+1)n+1,$$

and after dividing both sides by $p-1$, we can see that it is enough to have

$$p \geq n^2p^{1/2}+n(k-n+1). \tag{6}$$

To show that this holds, write $n = mk$ for some m with $0 < m < 1$. Then the right-hand side of (6) becomes

$$m^2k^2p^{1/2}+mk(k(1-m)+1) \leq m^2k^2p^{1/2}+2mk^2(1-m).$$

Since $p > k^4$, it suffices to show that

$$p^{1/2} > m^2p^{1/2}+2m(1-m).$$

But this is equivalent to having

$$p^{1/2} > 2-\frac{2}{m+1},$$

which is clearly true since $p > k^4$. This completes the proof of the lemma.

□

Lemma 15. *Suppose that the system* (3) *contains* $R = 3$ *congruences. If we can find 3 variables satisfying the hypotheses of Lemma 6, then we can contract them to a variable* T *such that any solution of* (3) *with* $T \not\equiv 0 \pmod{p}$ *will be nonsingular when traced back to the original* x*-variables. Moreover, we can guarantee that* T *has a nonzero coefficient in the degree* k_1 *congruence.*

Proof. The fact that it is possible to create the variable T comes from the conclusion of Lemma 6. We need to show now that we can do so in such a way that T has a nonzero coefficient in the degree k_1 congruence.

Let Z be the number of zeros of the degree k_1 congruence. By Lemma 12, we know that

$$|Z - p^2| \leq (k_1^2 - 3k_1 + 2)(p-1)p^{1/2},$$

which implies that

$$Z \leq p^2 + (k_1^2 - 3k_1 + 2)(p-1)p^{1/2}.$$

We also know from Lemma 7 that there are at least

$$(p - 1 - k_1 + k_2)(p - 1 - k_1 + k_3)$$

ways to choose t_2 and t_3 when creating T. If T has a zero coefficient in the degree k_1 congruence, then any nonzero value of T yields a solution of this congruence when traced back to the x-variables. If this is true for all possible ways to create T, then we find that there are at least

$$(p-1)(p - 1 - k_1 + k_2)(p - 1 - k_1 + k_3)$$

solutions of the degree k_1 congruence. Therefore, we are done if we can prove that

$$(p-1)(p-1-k_1+k_2)(p-1-k_1+k_3) > p^2 + (k_1^2 - 3k_1 + 2)(p-1)p^{1/2}. \quad (7)$$

Now, it is not hard to see that the left-hand side of (7) is strictly greater than $(p-k_1)^3$ and that the right-hand side of (7) is strictly less than $p^2 + k_1^2p^{3/2}$. Therefore it suffices to show that

$$(p - k_1)^3 > p^2 + k_1^2 p^{3/2}.$$

This is obviously true if and only if we have

$$(p - k_1)^3 - p^2 - k_1^2 p^{3/2} > 0.$$

If $k_1 = 3$, then this is true for all $p \geq 11$. For $k_1 \geq 4$, trivial algebra shows that it is sufficient to prove that

$$\left(p^3 - (3k_1 + 1)p^2 - k_1^2 p^{3/2}\right) + \left(3k_1^2 p - k_1^3\right) > 0.$$

We will show that both of the terms in large parentheses are positive. First, we have

$$\begin{aligned} p^3-(3k_1+1)p^2-k_1^2p^{3/2} &> p^3-(k_1^2+3k_1+1)p^2 \\ &> p^3-2k_1^2p^2 \\ &= p^2(p-2k_1^2). \end{aligned}$$

This final expression is positive since $p > k_1^4$. Also, since $p > k_1^4$, we clearly have $3k_1^2p - k_1^3 > 0$. This completes the proof of the lemma. □

Lemma 16. *Consider the system of congruences*

$$\begin{array}{rclcll} f(\mathbf{x}) & = & a_1x_1^k + a_2x_2^k + \cdots + a_8x_8^k & \equiv & 0 & \pmod{p} \\ g(\mathbf{x}) & = & b_1x_1^n + b_2x_2^n + \cdots + b_8x_8^n & \equiv & 0 & \pmod{p}, \end{array} \tag{8}$$

where $k > n$ and we assume that every coefficient is nonzero (modulo p). Suppose that $p > k^4$ and select any desired variable. Then there is a solution of (8) *in which the selected variable is nonzero.*

Proof. In this proof, we broadly follow the ideas in the proof of [18, Lemma 9]. Without loss of generality, suppose that the selected variable is x_8. Let N represent the total number of solutions of (8), and let M represent the total number of solutions with $x_8 \equiv 0 \pmod{p}$. We want to show that $N > M$. To do this, we will estimate both N and M by using exponential sums. For a prime p and any number x, we write $e_p(x)$ to mean

$$e_p(x) = \exp(2\pi i x/p).$$

Then it is well-known that

$$N = \frac{1}{p^2}\sum_{\mathbf{x}\in\mathbb{F}_p^8}\sum_{\alpha=0}^{p-1}\sum_{\beta=0}^{p-1} e_p(\alpha f(\mathbf{x}) + \beta g(\mathbf{x})).$$

If we define

$$T_j(\alpha,\beta) = \sum_{x_j=0}^{p-1} e_p(\alpha a_j x_j^k + \beta b_j x_j^n),$$

then we have

$$\begin{aligned} p^2 N &= \sum_{\alpha,\beta=0}^{p-1} T_1(\alpha,\beta)\cdots T_8(\alpha,\beta) \\ &= p^8 + \sum_{\substack{\alpha,\beta=0 \\ (\alpha,\beta)\neq(0,0)}}^{p-1} T_1(\alpha,\beta)\cdots T_8(\alpha,\beta). \end{aligned} \tag{9}$$

For ease of notation, we define $\sum^*_{\alpha,\beta}$ by

$$\sum_{\alpha,\beta}{}^{*} f(\alpha,\beta) = \sum_{\substack{\alpha,\beta=0 \\ (\alpha,\beta)\neq(0,0)}}^{p-1} f(\alpha,\beta).$$

With this new notation, we see that (9) implies that

$$\left|p^2N - p^8\right| \leq \sum_{\alpha,\beta}{}^{*} |T_1(\alpha,\beta)|\cdots|T_8(\alpha,\beta)|. \tag{10}$$

Applying Hölder's inequality to the right-hand side of (10), we find that

$$\left|p^2N - p^8\right| \leq \left(\sum_{\alpha,\beta}{}^{*} |T_1(\alpha,\beta)|^8\right)^{1/8} \cdots \left(\sum_{\alpha,\beta}{}^{*} |T_8(\alpha,\beta)|^8\right)^{1/8}.$$

Choose I so that the sum $\sum^*_{\alpha,\beta} |T_I(\alpha,\beta)|^8$ is as large as possible. Then we have

$$\begin{aligned} \left|p^2N - p^8\right| &\leq \sum_{\alpha,\beta}{}^{*} |T_I(\alpha,\beta)|^8 \\ &\leq \left(\sup_{(\alpha,\beta)\neq(0,0)} |T_I(\alpha,\beta)|\right)^4 \sum_{\alpha,\beta}{}^{*} |T_I(\alpha,\beta)|^4. \end{aligned} \tag{11}$$

Finally, we bound this last expression. By work of Wooley (see [18, Lemma 7]), we have

$$\sum_{\alpha,\beta=0}^{p-1} |T_I(\alpha,\beta)|^4 \leq knp^4. \tag{12}$$

This yields

$$\sum_{\alpha,\beta}^{*}|T_I(\alpha,\beta)|^4 = \left(\sum_{\alpha,\beta=0}^{p-1}|T_I(\alpha,\beta)|^4\right) - p^4 \le (kn-1)p^4.$$

Also, by the Riemann Hypothesis for finite fields (see for example [17, Chapter 2, Corollary 2.1]), we have

$$\sup_{(\alpha,\beta)\neq(0,0)}|T_I(\alpha,\beta)| \le (k-1)p^{1/2}. \tag{13}$$

Using these bounds, we obtain

$$\begin{aligned}\left|p^2N - p^8\right| &\le \left[(k-1)p^{1/2}\right]^4 \cdot (kn-1)p^4 \\ &= (k-1)^4(kn-1)p^6.\end{aligned}$$

This gives us the lower bound

$$N \ge p^6 - (k-1)^4(kn-1)p^4. \tag{14}$$

Now we need to find an upper bound for M. Note that solving (8) with $x_8 \equiv 0 \pmod{p}$ is the same thing as solving the system

$$\begin{array}{rcrcl} f^*(\mathbf{x}) & = & a_1x_1^k + a_2x_2^k + \cdots + a_7x_7^k & \equiv & 0 \pmod{p} \\ g^*(\mathbf{x}) & = & b_1x_1^n + b_2x_2^n + \cdots + b_7x_7^n & \equiv & 0 \pmod{p}. \end{array} \tag{15}$$

If M is the number of solutions of this system, then we proceed exactly as before to obtain

$$\begin{aligned}\left|p^2M - p^7\right| &\le \sum_{\alpha,\beta}^{*}|T_1(\alpha,\beta)|\cdots|T_7(\alpha,\beta)| \\ &\le \sum_{\alpha,\beta}^{*}|T_J(\alpha,\beta)|^7 \\ &\le \left(\sup_{(\alpha,\beta)\neq(0,0)}|T_J(\alpha,\beta)|\right)^3 \sum_{\alpha,\beta}^{*}|T_J(\alpha,\beta)|^4,\end{aligned}$$

where J is chosen such that $\sum_{\alpha,\beta}^{*}|T_J(\alpha,\beta)|^7$ is as large as possible. Using the estimates (12) and (13), we find that

$$\begin{aligned}\left|p^2M - p^7\right| &\le \left[(k-1)p^{1/2}\right]^3 \cdot (kn-1)p^4 \\ &= (k-1)^3(kn-1)p^{11/2}.\end{aligned}$$

This yields the upper bound

$$M \leq p^5 + (k-1)^3(kn-1)p^{7/2}. \tag{16}$$

From (14) and (16), we see that if we can show that

$$p^6 - (k-1)^4(kn-1)p^4 > p^5 + (k-1)^3(kn-1)p^{7/2}, \tag{17}$$

then it will follow that $N > M$, completing the proof. It suffices to show that

$$p^{5/2} - (k-1)^4(kn-1)p^{1/2} - p^{3/2} - (k-1)^3(kn-1) > 0.$$

Now, suppose that $p > k^4 > n^4$. It follows that $k-1 < p^{1/4}$ and $kn-1 < p^{1/2}$. Therefore, we have

$$\begin{aligned} p^{5/2} - (k-1)^4(kn-1)p^{1/2} - p^{3/2} - (k-1)^3(kn-1) \\ > \; p^{5/2} - p^2 - p^{3/2} - p^{5/4}. \end{aligned}$$

Hence it suffices to show that

$$p^{5/2} - p^2 - p^{3/2} - p^{5/4} > 0. \tag{18}$$

Since $p^2 > p^{3/2} > p^{5/4}$, (18) will be true whenever

$$p^{5/2} - 3p^2 > 0, \tag{19}$$

and it is easy to see that (19) is true whenever $p^{1/2} > 3$, i.e., whenever $p > 9$. However, since $k > n \geq 1$, we know that $k \geq 2$, and so $p > k^4 \geq 16$. This completes the proof of the lemma. □

4 Proof of Theorem 1

In this section, we give the proof of our first result, that for a system of two equations of degrees k and n, with $k > n$, having $s \geq 2k + 6n + 1$ variables guarantees a nontrivial p-adic solution when $p > k^4$.

Suppose that the system

$$\begin{aligned} a_1x_1^k + a_2x_2^k + \cdots + a_sx_s^k &= 0 \\ b_1x_1^n + b_2x_2^n + \cdots + b_sx_s^n &= 0 \end{aligned} \tag{20}$$

has exactly $s = 2k + 6n + 1$ variables. (If there are more variables than this, then we set the extra variables equal to zero.) By Lemma 4 with $r = 2$ and $|M_1| = 2k$, we may assume that

$$\begin{aligned} q_1 &\geq \Big(|M_1| + \frac{r}{2}\Big) \cdot \frac{1}{k} = 2 + \frac{1}{k} \\ q_2 &\geq \Big(s - |M_1| - r + \frac{r}{2}\Big) \cdot \frac{1}{n} = 6 \\ N &\geq \Big(|M_1| + \frac{r}{2}\Big) \cdot \frac{1}{k} + \Big(s - |M_1| - r + \frac{r}{2}\Big) \cdot \frac{1}{n} = 8 + \frac{1}{k}. \end{aligned}$$

Since these values must all be integers, we obtain

$$\begin{aligned} q_1 &\geq 3 \\ q_2 &\geq 6 \\ N &\geq 9. \end{aligned}$$

By renaming the variables if necessary, we may assume that $x_1, \ldots, x_N$ are the variables with at least one coefficient nonzero modulo p. We need to find a nonsingular solution of the system

$$\begin{aligned} a_1x_1^k + a_2x_2^k + \cdots + a_Nx_N^k &\equiv 0 \pmod{p} \\ b_1x_1^n + b_2x_2^n + \cdots + b_Nx_N^n &\equiv 0 \pmod{p}. \end{aligned} \tag{21}$$

We now divide the proof into two cases.

Case A: There are at least 3 variables with coefficient vector $\begin{pmatrix} * \\ 0 \end{pmatrix}$. Pick three variables whose coefficient vectors have this form and rename them x_1, x_2, and x_3. Since $q_2 \geq 6$, three of the remaining variables, which we label as x_4, x_5, and x_6, have coefficient vector $\begin{pmatrix} - \\ * \end{pmatrix}$. Set all other variables equal to zero. The system (21) now looks like

$$\begin{aligned} a_1x_1^k + \ a_2x_2^k + \ a_3x_3^k + \ a_4x_4^k + \ a_5x_5^k + \ a_6x_6^k &\equiv 0 \pmod{p} \\ b_4x_4^n + \ b_5x_5^n + \ b_6x_6^n &\equiv 0 \pmod{p}, \end{aligned}$$

where we know that $a_1, a_2, a_3, b_4, b_5, b_6 \not\equiv 0 \pmod{p}$. Since $p > k^4$, by Lemma 8 we can solve the bottom congruence with all three variables nonzero modulo p. After doing this, the degree k congruence takes the form

$$a_1x_1^k + a_2x_2^k + a_3x_3^k \equiv A \pmod{p}$$

for some number A. Again, Lemma 8 allows us to solve this equation with all three variables nonzero modulo p. We have now found a nontrivial solution of the system (21) and since $x_1, x_4 \not\equiv 0 \pmod{p}$, these two variables make the solution nonsingular. Thus we can find a solution to the original system (20) by Lemma 5.

Case B: There are fewer than 3 variables with coefficient vector $\begin{pmatrix} * \\ 0 \end{pmatrix}$. Suppose there are t such variables, and label them as $y_1, \ldots, y_t$ (if $t = 0$, then this does not result in any variables getting labels). Since $q_1 \geq 3$, there are at least $3 - t$ variables with coefficient vector $\begin{pmatrix} * \\ * \end{pmatrix}$. Pick $3 - t$ of these and for $i = 1, \ldots, 3 - t$, label them as $x_{3(i-1)+1}$. The remaining (at least 6) variables all have coefficient vector $\begin{pmatrix} - \\ * \end{pmatrix}$. Pick $2(3 - t)$ of these variables and label them as $x_{3(i-1)+2}, x_{3(i-1)+3}$ for $i = 1, \ldots, 3 - t$.

Now, we examine the system of congruences

$$\begin{array}{rcl} a_1x_1^k + a_2x_2^k + a_3x_3^k & \equiv & 0 \pmod{p} \\ b_1x_1^n + b_2x_2^n + b_3x_3^n & \equiv & 0 \pmod{p}. \end{array}$$

Here, we know that $a_1, b_1, b_2, b_3 \not\equiv 0 \pmod{p}$. By Lemma 14, there exists a number t_2 such that we can solve the congruence

$$b_1x_1^n + b_2x_2^n + b_3x_3^n \equiv 0 \pmod{p} \qquad (22)$$

with all three variables nonzero and with $x_2 = t_2x_1$, where the number t_2 satisfies the conclusion of Lemma 6. Suppose that this solution is $(x_1, x_2, x_3) = (\epsilon_1, \epsilon_2, \epsilon_3)$. If it happens that $a_1\epsilon_1^k + a_2\epsilon_2^k + a_3\epsilon_3^k \equiv 0 \pmod{p}$, then setting all other variables equal to zero gives a nonsingular solution of the system (21), and we are done. Otherwise, we set $(x_1, x_2, x_3) = (\epsilon_1T_1, \epsilon_2T_1, \epsilon_3T_1)$, where T_1 is a new variable. We note that any value of T_1 leads to a solution of (22), that T_1 has a nonzero coefficient in the degree k congruence, and that any solution of the system (21) with $T_1 \not\equiv 0 \pmod{p}$ will be nonsingular when traced back to the x-variables. (We acknowledge that we are abusing notation a bit by referring to the system (21) here even though we have really created a new system with our contraction. We trust that this will not cause the reader any confusion.) If $3 - t \geq 2$, then we repeat this argument with the variables x_4, x_5, x_6, obtaining a new variable T_2. If $3 - t = 3$, then we repeat it again with x_7, x_8, x_9, obtaining a new variable T_3.

At this point, we have a total of 3 variables labeled as either T_i or y_i for some i, and at least one of these is a T-variable. Moreover, all three of these variables have coefficient vector $\begin{pmatrix} * \\ 0 \end{pmatrix}$. Using these three variables, we can solve the degree k congruence with all variables nonzero. When traced back to the x-variables, this is a solution of the system (21), and since a T-variable is nonzero, this solution is nonsingular. This completes the proof of Case B, and hence completes the proof of Theorem 1.

5 Proof of Theorem 2

In this section, we give the proof of Theorem 2, that if $k_1 > k_2 > k_3$ and $p > k_1^4$, then we have $\Gamma_p^*(k_1, k_2, k_3) \leq 2k_1 + 14k_2 + 15k_3 + 1$.

Suppose that the system

$$\begin{array}{rcl} a_1x_1^{k_1} + a_2x_2^{k_1} + \cdots + a_sx_s^{k_1} & = & 0 \\ b_1x_1^{k_2} + b_2x_2^{k_2} + \cdots + b_sx_s^{k_2} & = & 0 \\ c_1x_1^{k_3} + c_2x_2^{k_3} + \cdots + c_sx_s^{k_3} & = & 0 \end{array} \tag{23}$$

has exactly $s = 2k_1 + 14k_2 + 15k_3 + 1$ variables. By Lemma 4 with $r = 4$, $|M_1| = 2k_1 - 1$, $|M_2| = 14k_2 - 1$, and $|M_3| = 15k_3 - 1$, and noting that q_1, q_2, q_3, q_{23} are all integers, we may assume that

$$\begin{array}{rcl} q_1 & \geq & 3 \\ q_2 & \geq & 15 \\ q_3 & \geq & 16 \\ q_{23} & \geq & 30. \end{array}$$

If $x_1, \ldots, x_N$ are the variables with at least one coefficient nonzero modulo p, then we need to find a nonsingular solution of the system

$$\begin{array}{rcl} f_1(\mathbf{x}) = a_1x_1^{k_1} + a_2x_2^{k_1} + \cdots + a_Nx_N^{k_1} & \equiv & 0 \pmod{p} \\ f_2(\mathbf{x}) = b_1x_1^{k_2} + b_2x_2^{k_2} + \cdots + b_Nx_N^{k_2} & \equiv & 0 \pmod{p} \\ f_3(\mathbf{x}) = c_1x_1^{k_3} + c_2x_2^{k_3} + \cdots + c_Nx_N^{k_3} & \equiv & 0 \pmod{p}. \end{array} \tag{24}$$

Again, we divide the proof into several cases. As with the proof of Theorem 1, the first case is simple. Unfortunately, the second case is more involved, requiring a number of subcases.

Case A: There are at least 3 variables with coefficient vector $\left(\begin{smallmatrix} * \\ 0 \\ 0 \end{smallmatrix}\right)$.
Choose three variables with this coefficient vector and label them as x_1, x_2, x_3. Note that these variables do not contribute to any of the numbers q_2, q_3, or q_{23}. Therefore we can find an additional set S of variables such that $q_2(S) \geq 3$, $q_3(S) \geq 6$, and $q_{23}(S) \geq 9$. (Recall from the discussion after the proof of Lemma 4 that for a set S of variables, $q_i(S)$ represents the number of variables in S that have a nonzero coefficient in the degree k_i congruence, and $q_{ij}(S)$ has a similar definition.) By (the proof of) Theorem 1, we can find a nonsingular solution of $f_2(\mathbf{x}) \equiv f_3(\mathbf{x}) \equiv 0 \pmod{p}$ using only the variables in S. After finding this solution, set all variables other than x_1, x_2, x_3, and the variables in S equal to zero. Then the degree k_2 and degree k_3 congruences will be zero for any values of x_1, x_2, x_3, and the degree k_1 congruence becomes

$$a_1 x_1^{k_1} + a_2 x_2^{k_1} + a_3 x_3^{k_1} \equiv A \pmod{p}$$

for some number A. Since $p > k_1^4$, we can solve this congruence with all three variables nonzero. This gives a solution of $f_1(\mathbf{x}) \equiv f_2(\mathbf{x}) \equiv f_3(\mathbf{x}) \equiv 0 \pmod{p}$, and this solution is nonsingular. Therefore, this solution lifts to a p-adic solution, completing the proof in this case.

Case B: There are fewer than 3 variables with coefficient vector $\left(\begin{smallmatrix} * \\ 0 \\ 0 \end{smallmatrix}\right)$.
The proof of this case is similar to the proof of Case B of Theorem 1. Pick 3 variables which have a nonzero coefficient in $f_1(\mathbf{x})$, and call them x_1, x_2, x_3. We now need to prove the following claim.

Claim. *In the situation above, we can divide the variables into pairwise disjoint sets S_1, S_2, S_3 such that for $i = 1, 2, 3$, we have $x_i \in S_i$ and such that in each set, we have*

$$\begin{aligned} q_2(S_i) &\geq 5 \\ q_3(S_i) &\geq 5 \\ q_{23}(S_i) &\geq 10. \end{aligned}$$

Proof of Claim. We will see how to choose the sets S_i. First, obviously, we add each x_i to S_i. Next note that since $q_{23} \geq 30$, if we can guarantee that each $q_2(S_i) \geq 5$ and $q_3(S_i) \geq 5$, while using at most 10 variables in each set, then we can "fill up" each set to 10 variables by using variables counted by q_{23}, thus ensuring that $q_{23}(S_i) \geq 10$. Hence, we will only worry about the conditions on $q_2(S_i)$ and $q_3(S_i)$.

Let σ be the number of variables in the set $\{x_1, x_2, x_3\}$ with coefficient vector either $\left(\begin{smallmatrix} * \\ * \\ - \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} * \\ - \\ * \end{smallmatrix}\right)$. Similarly, let σ_2 be the number of these variables with coefficient vector $\left(\begin{smallmatrix} * \\ * \\ 0 \end{smallmatrix}\right)$, let σ_3 be the number of these variables with coefficient vector $\left(\begin{smallmatrix} * \\ 0 \\ * \end{smallmatrix}\right)$, and σ_{23} be the number of these variables with coefficient vector $\left(\begin{smallmatrix} * \\ * \\ * \end{smallmatrix}\right)$. Note that we have $\sigma = \sigma_2 + \sigma_3 + \sigma_{23}$, and $1 \leq \sigma \leq 3$. Since $q_{23} \geq 30$, we still have $27 \leq 30 - \sigma \leq 29$ variables whose coefficient vector is not $\left(\begin{smallmatrix} - \\ 0 \\ 0 \end{smallmatrix}\right)$ That is, there are $30 - \sigma$ variables with a nonzero coefficient in either the 2nd or 3rd equation. Write δ for the number of these variables whose coefficient vector is $\left(\begin{smallmatrix} - \\ * \\ * \end{smallmatrix}\right)$,

Suppose first that $\delta \geq 15 - \sigma_{23}$. Then we can add $15 - \sigma_{23}$ of these variables to the sets S_i in such a way that each set has 5 variables with coefficient vector $\left(\begin{smallmatrix} - \\ * \\ * \end{smallmatrix}\right)$. This guarantees that $q_2(S_i), q_3(S_i) \geq 5$ for each i. At this point, each set contains at most 6 variables, and so we are done by the remarks at the beginning of the proof.

Next, suppose that $\delta \leq 12$. Distribute the variables with coefficient vector $\left(\begin{smallmatrix} - \\ * \\ * \end{smallmatrix}\right)$ as equally as possible among the sets. At this point, each set has $q_2(S_i), q_3(S_i) \leq 5$. Since there are $q_2 - \delta - \sigma_2 - \sigma_{23} \geq 15 - (\delta + \sigma_2 + \sigma_{23})$ remaining variables with coefficient vector $\left(\begin{smallmatrix} - \\ * \\ 0 \end{smallmatrix}\right)$, we can add enough variables of this type to each set to guarantee that $q_2(S_i) = 5$ for each set. Similarly, we have $q_3 - \delta - \sigma_3 - \sigma_{23} \geq 16 - (\delta + \sigma_3 + \sigma_{23})$ variables remaining with coefficient vector $\left(\begin{smallmatrix} - \\ 0 \\ * \end{smallmatrix}\right)$. Since we currently have $q_3(S_i) \leq 5$ for each i, we can add enough variables of this type to each set so that we have $q_3(S_i) = 5$ for each set. At this point, each set has $q_2(S_i) = q_3(S_i) = 5$, and has at most 10 variables in total. Hence we are done by the remarks at the beginning of the proof.

This leaves possible cases with $\delta = 14$ and $\delta = 13$. Suppose first that $\delta = 14$. Then we may assume that $\sigma_{23} = 0$. Let T be the set of variables not counted by either σ or δ. Then all the variables in T have a coefficient vector of either $\begin{pmatrix} - \\ * \\ 0 \end{pmatrix}$ or $\begin{pmatrix} - \\ 0 \\ * \end{pmatrix}$. If T contains variables of both types, then we may partition the variables counted by δ into three groups of 5, 5, and 4 variables, and add them to S_1, S_2, and S_3, respectively. Then we either have $q_2(S_3) = 4$ and $q_3(S_3) = 5$, or we have $q_2(S_3) = 5$ and $q_3(S_3) = 4$. In either case, we may add a single variable from T to guarantee that the conditions on $q_2(S_3)$ and $q_3(S_3)$ are satisfied. As before, we are done by the remarks at the beginning of the proof.

If $\delta = 14$ and the set T contains only variables of coefficient vector $\begin{pmatrix} - \\ * \\ 0 \end{pmatrix}$, then since $q_3 \geq 16$, we must have $\sigma_3 \geq 2$. Suppose without loss of generality that S_3 contains a variable counted by σ_3. Partition the variables counted by δ into three sets of sizes 5, 5, and 4, and add them to S_1, S_2, and S_3, making sure that the 4-variable block is added to S_3. Then we have $q_2(S_3) = 4$ and $q_3(S_3) = 5$. Adding one variable from T to S_3 now guarantees that for each set, the conditions on $q_2(S_i)$ and $q_3(S_i)$ are satisfied, and we can finish as before. On the other hand, if T contains only variables with coefficient vector $\begin{pmatrix} - \\ 0 \\ * \end{pmatrix}$, then since $q_2 \geq 15$, we must have $\sigma_2 \geq 1$. Suppose that S_3 contains a variable counted by σ_2. When we add the variables counted by δ, we again mandate that the 4-variable block of the partition is added to S_3. As before, we may then add a variable from T to S_3, guaranteeing that all the conditions on each $q_2(S_i)$ and $q_3(S_i)$ are satisfied, and finish as before.

Finally, we have the case $\delta = 13$. This case can be handled in essentially the same way as the $\delta = 14$ case. This time, we either have $\sigma_{23} = 0$ or $\sigma_{23} = 1$. If T contains at least two variables of each coefficient class $\begin{pmatrix} - \\ * \\ 0 \end{pmatrix}$ and $\begin{pmatrix} - \\ 0 \\ * \end{pmatrix}$, then we proceed as in the $\delta = 14$ case. The situation in which T has at most one variable of one of the two types can also be treated as above by partitioning the variables counted by δ into blocks of sizes 5, 4, and 4, and being careful about putting the 4-variable blocks into appropriate sets. We omit the details. □

Now that the claim is proved, we can finish the proof of Case B. For $i = 1, 2, 3$, if it happens that x_i has coefficient vector $\left(\begin{smallmatrix}*\\0\\0\end{smallmatrix}\right)$, then we set $x_i = U_i$. Otherwise, we will show that using the variables in S_i, we can create a new variable U_i such that U_i has coefficient vector $\left(\begin{smallmatrix}-\\0\\0\end{smallmatrix}\right)$ and also has the property that any solution of the system (24) with $U_i \not\equiv 0 \pmod{p}$ is nonsingular when traced back to the x-variables. Assume for the moment that this has already been done. If U_i actually has coefficient vector $\left(\begin{smallmatrix}0\\0\\0\end{smallmatrix}\right)$, then setting all other variables equal to zero gives a nonsingular solution of (24), and we are finished. Hence we will always assume that U_i has coefficient vector $\left(\begin{smallmatrix}*\\0\\0\end{smallmatrix}\right)$.

Once we create the U-variables, we set any x-variables that we have not yet used equal to 0. Then as in the proof of Case A, we will have $f_2(\mathbf{x}) \equiv f_3(\mathbf{x}) \equiv 0 \pmod{p}$ regardless of the values of U_1, U_2, U_3, and the degree k_1 congruence looks like

$$A_1U_1^{k_1} + A_2U_2^{k_1} + A_3U_3^{k_1} \equiv A \pmod{p}$$

for some numbers A_1, A_2, A_3, A. Since $p > k_1^4$, we can solve this final congruence with all of the U_i nonzero, and at least one of these nonzero values guarantees that this solution is nonsingular, leading to a p-adic solution. It remains to show that the required variables U_i can always be constructed.

We construct the variables U_i in the following manner. Let S be one of the sets S_i. Among the variables in S, we can find one that has a nonzero coefficient in $f_1(\mathbf{x})$, another that has a nonzero coefficient in $f_2(\mathbf{x})$, and a third that has a nonzero coefficient in $f_3(\mathbf{x})$. By Lemma 15, we can contract these to a variable T that has coefficient vector $\left(\begin{smallmatrix}*\\-\\-\end{smallmatrix}\right)$ and has the property that any solution of (24) with $T \not\equiv 0 \pmod{p}$ must be nonsingular when traced back to the x-variables. Clearly, any variable made through a contraction using T also has this property. Thus, it remains to show that we can use T in a contraction of variables resulting in a new variable U with coefficient vector $\left(\begin{smallmatrix}*\\0\\0\end{smallmatrix}\right)$.

For this, we need to split the proof up into several cases. Let S^* be the set containing the x-variables in S that were not used to create T. Then we must have

$$\begin{aligned} q_2(S^*) &\geq 2 \\ q_3(S^*) &\geq 2 \\ q_{23}(S^*) &\geq 7. \end{aligned}$$

Case B.1: T has coefficient vector $\left(\begin{smallmatrix} * \\ 0 \\ 0 \end{smallmatrix}\right)$.
In this case we simply set $U = T$, and we are done.

Case B.2: T has coefficient vector $\left(\begin{smallmatrix} * \\ * \\ 0 \end{smallmatrix}\right)$.
We split this case into subcases as follows.
Case B.2.a: There are at least two variables in S^* with coefficient vector $\left(\begin{smallmatrix} - \\ * \\ 0 \end{smallmatrix}\right)$.
Call these two variables y_1 and y_2 and set all other variables in S^* equal to 0. Then the variables T, y_1, y_2 have coefficient vectors

$$\left(\begin{smallmatrix} * \\ * \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} - \\ * \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} - \\ * \\ 0 \end{smallmatrix}\right)$$

respectively. We can solve the degree k_2 congruence with all three of these variables nonzero, and by Lemma 13, we can do this in a way that is not a solution of the degree k_1 congruence. Thus we can contract T, y_1, y_2 to a new variable U with coefficient vector $\left(\begin{smallmatrix} * \\ 0 \\ 0 \end{smallmatrix}\right)$, as desired.

Case B.2.b: At most one variable in S^* has coefficient vector $\left(\begin{smallmatrix} - \\ * \\ 0 \end{smallmatrix}\right)$.
Among the variables in S^*, we have at least one with coefficient vector $\left(\begin{smallmatrix} - \\ * \\ * \end{smallmatrix}\right)$ and at least five additional variables with coefficient vector $\left(\begin{smallmatrix} - \\ - \\ * \end{smallmatrix}\right)$. If there are two with coefficient vector $\left(\begin{smallmatrix} - \\ * \\ * \end{smallmatrix}\right)$, then we can make two groups of three variables each, with coefficient vectors

$$\left(\begin{smallmatrix} - \\ * \\ * \end{smallmatrix}\right), \left(\begin{smallmatrix} - \\ - \\ * \end{smallmatrix}\right), \left(\begin{smallmatrix} - \\ - \\ * \end{smallmatrix}\right) \qquad \text{and} \qquad \left(\begin{smallmatrix} - \\ * \\ * \end{smallmatrix}\right), \left(\begin{smallmatrix} - \\ - \\ * \end{smallmatrix}\right), \left(\begin{smallmatrix} - \\ - \\ * \end{smallmatrix}\right),$$

while if there is only one variable with coefficient vector $\left(\begin{smallmatrix} - \\ * \\ * \end{smallmatrix}\right)$, then we can make two groups of three variables each, with coefficient vectors

$$\left(\begin{smallmatrix} - \\ * \\ * \end{smallmatrix}\right), \left(\begin{smallmatrix} - \\ - \\ * \end{smallmatrix}\right), \left(\begin{smallmatrix} - \\ - \\ * \end{smallmatrix}\right) \qquad \text{and} \qquad \left(\begin{smallmatrix} - \\ - \\ * \end{smallmatrix}\right), \left(\begin{smallmatrix} - \\ - \\ * \end{smallmatrix}\right), \left(\begin{smallmatrix} - \\ - \\ * \end{smallmatrix}\right).$$

In the first three of these groups, we can solve the degree k_3 congruence in such a way that the degree k_2 polynomial is nonzero. If we are in a situation where the last group exists, then we do actually have a variable with coefficient vector $\begin{pmatrix} - \\ * \\ 0 \end{pmatrix}$. Using the variables in this last group, we can solve the degree k_3 congruence. If that solution happens to make the degree k_2 congruence equal 0, then we add the variable of coefficient vector $\begin{pmatrix} - \\ * \\ 0 \end{pmatrix}$ to the group and set it equal to 1. This gives a solution of the degree k_3 congruence which is not a solution of the degree k_2 congruence.

Using these solutions, we can form contractions to make two variables T_1 and T_2 with coefficient vector $\begin{pmatrix} - \\ * \\ 0 \end{pmatrix}$. Then, using the variables T, T_1, and T_2, we can solve the degree k_2 congruence with all three variables nonzero and such that the degree k_1 congruence is also nonzero. Then these three variables contract to a new variable U with coefficient vector $\begin{pmatrix} * \\ 0 \\ 0 \end{pmatrix}$, as desired. This completes the proof of Case B.2.

Case B.3: T has coefficient vector $\begin{pmatrix} * \\ 0 \\ * \end{pmatrix}$.
The proof of this case proceeds exactly like the proof of Case B.2, switching the roles of the degree k_2 and degree k_3 congruences. So for example, Case B.3.a would be the case in which there are at least two variables in S^* with coefficient vector $\begin{pmatrix} - \\ 0 \\ * \end{pmatrix}$. We omit the rest of the details of this case.

Case B.4: T has coefficient vector $\begin{pmatrix} * \\ * \\ * \end{pmatrix}$.
Again, we split this case into several subcases.

Case B.4.a: The set S^* contains two variables with coefficient vector $\begin{pmatrix} - \\ * \\ 0 \end{pmatrix}$. Since $q_3(S^*) \geq 2$, we can find a set of three variables which includes T such that all have nonzero coefficients in $f_3(\mathbf{x})$. Then we can use these three variables to find a solution of $f_3(\mathbf{x}) \equiv 0 \pmod{p}$ in which all three variables are nonzero and which is also not a solution of the degree k_2 congruence. These variables can then be contacted to a new variable T^* with coefficient vector $\begin{pmatrix} - \\ * \\ 0 \end{pmatrix}$. Using T^* and two other variables with this same coefficient vector, we can solve the congruence $f_2(\mathbf{x}) \equiv 0 \pmod{p}$. Then these variables contract to a new variable U with coefficient vector $\begin{pmatrix} * \\ 0 \\ 0 \end{pmatrix}$, as desired.

Case B.4.b: The set S^* contains two variables with coefficient vector $\begin{pmatrix} - \\ 0 \\ * \end{pmatrix}$. In this case, we proceed in the same manner as in the proof of Case B.4.a, with the roles of the degree k_2 and degree k_3 congruences interchanged. We omit the details.

Case B.4.c: We are not in any of the other cases.
If none of the other cases apply, then we have at most 1 variable with coefficient vector $\begin{pmatrix} - \\ * \\ 0 \end{pmatrix}$ and at most 1 with coefficient vector $\begin{pmatrix} - \\ 0 \\ * \end{pmatrix}$. Therefore, there are at least 5 variables with coefficient vector $\begin{pmatrix} - \\ * \\ * \end{pmatrix}$.

Subcase B.4.c.1: There is a variable in S^* with coefficient vector $\begin{pmatrix} - \\ * \\ 0 \end{pmatrix}$. Call this variable y. We can find a set of six variables, which includes T, all of which have coefficient vector $\begin{pmatrix} - \\ * \\ * \end{pmatrix}$. Divide these into two subsets of three variables each. In each subset, we can solve the congruence $f_3(\mathbf{x}) \equiv 0 \pmod{p}$ with all three variables nonzero, and do it in such a way that $f_2(\mathbf{x}) \not\equiv 0 \pmod{p}$. Contracting the variables in each subset, we can create two new variables T_1 and T_2 with coefficient vector $\begin{pmatrix} - \\ * \\ 0 \end{pmatrix}$. With these variables and y, we can solve the congruence $f_2(\mathbf{x}) \equiv 0 \pmod{p}$. Using this solution, we can contract T_1, T_2, y to a new variable U with coefficient vector $\begin{pmatrix} * \\ 0 \\ 0 \end{pmatrix}$, as desired.

Subcase B.4.c.2: There is a variable in S^* with coefficient vector $\begin{pmatrix} - \\ 0 \\ * \end{pmatrix}$. The proof of this subcase proceeds in the same manner as the previous subcase, with the roles of f_2 and f_3 interchanged. We omit the details.

Subcase B.4.c.3: Every variable in S^* has coefficient vector $\begin{pmatrix} - \\ * \\ * \end{pmatrix}$.
In this case, we have (including T), eight variables with coefficient vector $\begin{pmatrix} - \\ * \\ * \end{pmatrix}$. By Lemma 16, we can use these variables to find a solution of the system $f_2(\mathbf{x}) \equiv f_3(\mathbf{x}) \equiv 0 \pmod{p}$ in which $T \not\equiv 0 \pmod{p}$. If we contract the variables used in this solution, we obtain a new variable U with coefficient vector $\begin{pmatrix} * \\ 0 \\ 0 \end{pmatrix}$, as desired. This completes the proof of this final subcase, and hence completes the proof of Theorem 2.

Remark 17. For use in the proof of Theorem 3 in the next section, we make a few comments on this proof. First, we note that although we knew that $q_3 \geq 16$ due to normalization, we only used the fact that $q_3 \geq 15$. Even in the proof of the claim at the beginning of Case B, we really only needed to have $q_3 \geq 15$. The "extra" variable counted by q_3 came from making s large enough to guarantee that $q_{23} \geq 30$ in addition to the bounds on the other q_i. Next, we mention that when we made a T-variable in Case B, we assumed as a worst-case scenario that the x-variables used to make it all had coefficient vector $\begin{pmatrix} * \\ * \\ * \end{pmatrix}$. Thus, if S^{**} represents the set of x-variables remaining after making a single T-variable, then we have

$$\begin{aligned} q_1(S^{**}) &\geq 2 \\ q_2(S^{**}) &\geq 12 \\ q_3(S^{**}) &\geq 12 \\ q_{23}(S^{**}) &\geq 27. \end{aligned}$$

Finally, we note that in our proof, we showed that a T-variable can always be used in the solution to the system (24). That is, if T_i is one of the T-variables, then we can find a solution of (24) in which $T_i \not\equiv 0 \pmod{p}$. One consequence of this is that we have shown that (given the conditions on q_1, q_2, q_3, q_{23}) any specified variable with coefficient vector $\begin{pmatrix} * \\ - \\ - \end{pmatrix}$ can be used with nonzero value in a solution of (24).

6 Proof of Theorem 3

In this section, we give the proof of Theorem 3. As discussed in the introduction, our goal in this section is to obtain a single bound for $\Gamma_p^*(k_1, \ldots, k_R)$ that works for any number of equations (provided $p > k_1^4$), and not to find the smallest possible bound that we can. Our strategy for the proof is slightly different than in the proofs of Theorem 1 and Theorem 2. In those proofs, we aimed to produce variables U_1, U_2, U_3 which had nonzero coefficients in only the degree k_1 equation and also so that at least one of them had the property that a solution with $U_i \not\equiv 0 \pmod{p}$ would necessarily lead to a nonsingular solution of the system of congruences associated with (1). For the proof of Theorem 3, we still make U-variables which guarantee nonsingular solutions of congruences, but instead of using them to solve only the degree k_1 congruence, we use them to solve the subsystem of congruences of degrees $k_1, k_2, \ldots, k_{R-3}$. The final three congruences are handled by an appeal to (the proof of) Theorem 2.

To prove Theorem 3, suppose that s is equal to the bound in the statement of the theorem. Let $r = R+1$. For $1 \leq i \leq R-3$, set $|M_i| = (i \cdot 3^{R-3}-1)k_i-1$, and let

$$\begin{aligned} |M_{R-2}| &= ((R+1) \cdot 3^{R-3} - 1)k_{R-2} - 1 \\ |M_{R-1}| &= ((R+14) \cdot 3^{R-3} - 1)k_{R-1} - 1 \\ |M_R| &= ((R+30) \cdot 3^{R-3} - 1)k_R - 1. \end{aligned}$$

By Lemma 4, using these values of r and $|M_i|$, we may assume that

$$\begin{aligned} q_i &\geq i \cdot 3^{R-3} \qquad (1 \leq i \leq R-3) \\ q_{R-2} &\geq (R+1) \cdot 3^{R-3} \\ q_{R-1} &\geq (R+14) \cdot 3^{R-3} \\ q_R &\geq (R+30) \cdot 3^{R-3}. \end{aligned}$$

Suppose that $x_1, \ldots, x_N$ are the variables that appear with a nonzero coefficient in at least one of the forms. Then we need to find a nonsingular solution of the system of congruences

$$\begin{array}{lcll} f_1(\mathbf{x}) = a_{11}x_1^{k_1} + a_{12}x_2^{k_1} + \cdots + a_{1N}x_N^{k_1} & \equiv & 0 & \pmod{p} \\ f_2(\mathbf{x}) = a_{21}x_1^{k_2} + a_{22}x_2^{k_2} + \cdots + a_{2N}x_N^{k_2} & \equiv & 0 & \pmod{p} \\ & \vdots & & \\ f_R(\mathbf{x}) = a_{R1}x_1^{k_R} + a_{R2}x_2^{k_R} + \cdots + a_{RN}x_N^{k_R} & \equiv & 0 & \pmod{p}. \end{array} \tag{25}$$

Now we make 3^{R-3} disjoint sets $S_1, \ldots, S_{3^{R-3}}$ of variables as follows. There are at least 3^{R-3} variables with a nonzero coefficient in f_1, and we put one of these into each set. Of the remaining variables, there are still at least 3^{R-3} which have a nonzero coefficient in f_2, and we put one of these into each set. We repeat this procedure with $f_3, f_4, \ldots, f_{R-3}$. After this, we still have at least $4 \cdot 3^{R-3}$ variables remaining which have nonzero coefficients in f_{R-2}, and we add four of these to each set. Similarly, we can add an additional 13 variables to each set which have nonzero coefficients in f_{R-1}, and then an additional 16 variables to each set which have nonzero coefficients in f_R.

Let S be one of the sets S_i. Using one variable in S from each stage of the above procedure, Lemma 6 allows us to make a contraction to a new variable T having the property that any solution of (25) with $T \not\equiv 0 \pmod{p}$ will be nonsingular. If it happens that the coefficient of T in f_{R-2} is zero, then we take one of the variables from the f_{R-2} stage of adding variables to S and also set that variable equal to T. Then T still has the property that any solution of (25) with $T \not\equiv 0 \pmod{p}$ is nonsingular, and also has a nonzero coefficient in f_{R-2}.

Let S^* be the set of x-variables remaining in S after the variable T is constructed, and note that we have $q_{R-2}(S^*) \geq 2$, $q_{R-1}(S^*) \geq 12$, $q_R(S^*) \geq 15$, and $q_{R-1,R}(S^*) \geq 27$. By the remark after the proof of Theorem 2, we can find a solution of the system $f_{R-2}(\mathbf{x}) \equiv f_{R-1}(\mathbf{x}) \equiv f_R(\mathbf{x}) \equiv 0 \pmod{p}$ in which $T \not\equiv 0 \pmod{p}$. Then the variables used in this solution can be contracted to a new variable U. This variable has the property that any solution of (25) with $U \not\equiv 0 \pmod{p}$ is nonsingular and also the property that any value of U provides a solution of $f_{R-2}(\mathbf{x}) \equiv f_{R-1}(\mathbf{x}) \equiv f_R(\mathbf{x}) \equiv 0 \pmod{p}$.

If we apply this procedure to all the sets S_i, $i = 1, \ldots, 3^{R-3}$, then we obtain variables U_i, $i = 1, \ldots, 3^{R-3}$ with the properties in the preceding paragraph. By Lemma 9, we can use these variables to find a nontrivial solution of the system $f_1(\mathbf{x}) \equiv \cdots \equiv f_{R-3}(\mathbf{x}) \equiv 0 \pmod{p}$. The properties of the U_i guarantee that this yields a solution of (25). Since at least one of the U_i is nonzero, this solution of (25) is nonsingular when traced back to the original x-variables. This solution lifts to a p-adic solution by Hensel's lemma, completing the proof of the theorem.

7 Acknowledgements

Michael Knapp was supported by FAPEG Programa Pesquisador Visitante Estrangeiro 2024. Much of this work was completed during a visit by the first author at the Instituto de Matemática e Estatística at the Universidade Federal de Goiás, whose warm hospitality is greatly appreciated. The authors would also like to thank Dr. Timothy Clark (Loyola University Maryland) for a very helpful discussion about algebraic geometry.

References

[1] G. I. Arkhipov and A. A. Karatsuba, *“A problem of comparison theory”*, Uspekhi Mat. Nauk **37** (1982), 161–162 (Russian).

[2] O. D. Atkinson, J. Brüdern, and R. J. Cook, *Simultaneous additive congruences to a large prime modulus*, Mathematika **39** (1992), no. 1, 1–9.

[3] E. Artin, *Collected papers*, Addison-Wesley Pub. Co., Reading, Mass., 1965.

[4] W. D. Brownawell, *“On p-adic zeros of forms”*, J. Number Theory **18** (1984), 342–349.

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

[6] M. Dodson, *“Homogeneous additive congruences”*, Philos. Trans. Roy. Soc. London Ser. A **261** (1967), 163–210.

[7] Germain, *$x^2 + y^2 + z^2$ is irreducible in $\mathbb{C}[x, y, z]$*, Mathematics Stack Exchange. https://math.stackexchange.com/questions/486668/x2-y2-z2-is-irreducible-in-mathbb-c-x-y-z. (Accessed November 14, 2025).

[8] Hemar Godinho and Paulo H. A. Rodrigues, *On p-adic zeros of systems of diagonal forms restricted by a congruence condition*, J. Théor. Nombres Bordeaux **19** (2007), no. 1, 205–219.

[9] M. J. Greenberg, *Lectures on forms in many variables*, W. A. Benjamin and Co., New York, 1969.

[10] M. Knapp, *“Systems of diagonal equations over p-adic fields”*, J. London Math. Soc. (2) **63** (2001), 257–267.

[11] M. Knapp, *“On systems of diagonal forms”*, J. Aust. Math. Soc. **82** (2007), 221–236.

[12] Michael P. Knapp, *On systems of diagonal forms. II*, Math. Proc. Cambridge Philos. Soc. **147** (2009), no. 1, 31–45.

[13] D. B. Leep and W. M. Schmidt, *"Systems of homogeneous equations"*, Invent. Math. **71** (1983), 539–549.

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

[15] Lidl, R., and Niederreiter, H., *Finite fields*, Encyclopedia of Mathematics and its Applications, Vol. 20, 2nd Ed, Cambridge University Press, Cambridge, 1997.

[16] Ivan D. Meir, *Pairs of additive congruences to a large prime modulus*, J. Number Theory **63** (1997), no. 1, 132–142.

[17] Wolfgang Schmidt, *Equations over finite fields: an elementary approach*, second ed., Kendrick Press, Heber City, UT, 2004.

[18] T. D. Wooley, *"On simultaneous additive equations III"*, Mathematika **37** (1990), 85–96.

[19] ______, *"Artin's conjecture and systems of diagonal equations"*, Forum Math. **27** (2015), 2259–2265.