Mathematika 66 (2020) 577–611 doi:10.1112/mtk.12030

BEYOND ARTIN'S CONJECTURE FOR CUBIC FORMS

MIRIAM SOPHIE KAESBERG

Abstract. It is established that every cubic form in at least eight variables which can be realised as a diagonal form on a hyperplane has a non-trivial p-adic solution for all primes p.

§1. *Introduction.* Artin [1] expected that every form of degree k with integer coefficients in s variables has a non-trivial p-adic solution for all primes p provided $s > k^2$. Even though this conjecture has been proven wrong in general, there are special cases in which it is true. Until today the only cases known are those with $k = 1$, $k = 2$ and $k = 3$, the last of which was proven by Lewis [7].

Here, I follow an idea by Brüdern and Robert [2] who presented an approach which provides a way to prove Artin's conjecture for some cases. Their approach is based on the following lemma, a special case of the proposition in [2, Section 2], where it is proven that solving a form of degree k is equivalent to solving a particular system of diagonal forms.

LEMMA 1. *For a form $g \in \mathbb{Q}[X_1, \dots, X_s]$ of degree k, there exist r linear forms $L_j \in \mathbb{Q}[Y_1, \dots, Y_{r+s}]$ $(1 \leqslant j \leqslant r)$ and $r + s$ coefficients $c_j \in \mathbb{Q}$ $(1 \leqslant j \leqslant r + s)$ for an r between 0 and $\frac{s(s+1)\dots(s+k-1)}{k!}$ with the property that the equation $g(x_1, \dots, x_s) = 0$ has a solution $\mathbf{x} \in \mathbb{Q}_p^s \backslash \{\mathbf{0}\}$ if and only if the system of equations*

$$\sum_{j=1}^{r+s} c_j y_j^k = 0, \qquad L_j(\mathbf{y}) = 0 \qquad (1 \leqslant j \leqslant r)$$

has a solution $\mathbf{y} \in \mathbb{Q}_p^{r+s} \backslash \{\mathbf{0}\}$.

Applying Lemma 1 with $s = k^2 + 1$ shows that if for every $0 \leqslant r \leqslant \frac{(k^2+1)(k^2+2)\dots(k^2+k)}{k!}$ the system

$$\sum_{j=1}^{k^2+r+1} a_j x_j^k = \sum_{j=1}^{k^2+r+1} b_{ij} x_j = 0 \qquad (1 \leqslant i \leqslant r),$$

consisting of one diagonal form of degree k and r linear diagonal forms in $k^2 + r + 1$ variables with integer coefficients a_j and b_{ij} has a non-trivial p-adic solution for all primes p, then every form of degree k with at least $k^2 + 1$ variables has one.

For $k = 3$, this implies that every form of degree 3 with at least 10 variables has a non-trivial p-adic solution for all primes p if and only if for a specific $0 \leqslant r \leqslant 220$ and integer coefficients a_j and b_{ij} the system

$$\sum_{j=1}^{10+r} a_j x_j^3 = \sum_{j=1}^{10+r} b_{ij} x_j = 0 \qquad (1 \leqslant i \leqslant r) \tag{1.1}$$

Received 3 September 2019, published online 4 May 2020.
MSC (2010): 11D72 (primary), 11E76 (secondary).

has a non-trivial p-adic solution for all primes p. The case $r = 0$ was proven by Lewis [8]. He even showed that every equation of the form

$$\sum_{i=1}^{s} a_i x_i^3 = 0, \qquad a_i \in \mathbb{Z},$$

has a non-trivial p-adic solution for all p if $s \geqslant 7$. This includes the case $r = 0$, but it is by three variables better than required. It is the aim of this paper to prove that for $r = 1$ one does not lose this advantage of three variables.

THEOREM 1. *Let $s \geqslant 8$ and $a_i, b_i \in \mathbb{Z}$ for $1 \leqslant i \leqslant s$. Then the system*

$$\sum_{j=1}^{s} a_j x_j^3 = \sum_{j=1}^{s} b_j x_j = 0, \tag{1.2}$$

has a solution $(x_1, \dots, x_s) \in \mathbb{Q}_p^s \backslash \{\mathbf{0}\}$ for all p prime.

It is impossible for all systems

$$\sum_{j=1}^{7+r} a_j x_j^3 = \sum_{j=1}^{7+r} b_{ij} x_j = 0 \qquad (1 \leqslant i \leqslant r)$$

with integer coefficients a_j and b_{ij} to have a non-trivial p-adic solution for all primes p and all $0 \leqslant r \leqslant 220$. Otherwise it would follow from Lemma 1 that every form of degree 3 with integer coefficients in at least seven variables has a non-trivial p-adic solution for all primes p. But as it was proven by Mordell [9] that Artin's conjecture is strict for $k = 3$, that is, there exist a cubic form of degree 3 in nine variables and a prime p without a non-trivial p-adic solution, somewhere between $r = 0$ and $r = 220$ this gap of three variables is closed.

The proof of Theorem 1 will follow a pattern by Brüdern and Robert [2]. Dividing the set of primes into sets depending on their residue class modulo 3, those primes congruent to 2 modulo 3 will be worked on in § 2 using the contraction argument by Brüdern and Robert [2, Section 3] and some work of Dodson [5]. For the remaining primes, the version of Hensels's Lemma in § 3, established by Brüdern and Robert [2, Section 4], will give a combinatorial approach to the problem, which indicates a necessity to distinguish between primes congruent to 1 modulo 3 and the prime three. Section 4 will introduce an equivalence relation on the set of system, which Brüdern and Robert [2, Section 6] used to pick representative with good properties. In § 5, I will prove with a simple combinatorial approach for primes congruent to 1 modulo 3 that most cases have a non-trivial p-adic solution. The remaining cases will be handled in §§ 6, 7 using a more complex approach of Brüdern and Robert [2, Sections 8 and 9] in § 6 and a result by Leep and Yeoman [6] on the number of solutions of an absolute irreducible polynomial in both sections. The proof will be completed in § 8 where combinatorial methods are used to show the existence of non-trivial 3-adic solutions.

§2. *The case* $p \equiv 2 \bmod 3$.

In this section, I prove Theorem 1 for primes p congruent to 2 modulo 3. These primes are relatively easy to handle since the set of cubic residue classes modulo p equals the set of all residue classes modulo p. Hence, the equation

$$c_1 x_1^3 + \cdots + c_t x_t^3 = 0, \tag{2.1}$$

in which all coefficients are integers, has a non-trivial p-adic solution even if t is relatively small for primes p congruent to 2 in comparison to primes p congruent to 1 modulo 3. Dodson

[5] denoted the smallest t such that a non-trivial p-adic solution exists for all equations (2.1) by $\Gamma^*(3, p)$. More general, $\Gamma^*(k, p)$ denotes the smallest number $t \in \mathbb{N}$, such that for all $c_1, \dots, c_t \in \mathbb{Z}$ the equation

$$c_1 x_1^k + \dots + c_t x_t^k = 0$$

has a solution $\mathbf{x} \in \mathbb{Q}_p^t \backslash \{\mathbf{0}\}$. The problem of showing that a system (1.2) has a non-trivial p-adic solution was broken down by Brüdern and Robert [2, Section 3] into a restriction on $\Gamma^*(k, p)$ depending on s.

LEMMA 2. *Suppose* $s \geqslant 2\Gamma^*(k, p)$. *Then the system* (1.2) *has a non-trivial solution in* $\mathbb{Q}_p$.

Proof. See [2, Lemma 3.1]. □

All that remains to be shown is that $\Gamma^*(3, p) \leqslant 4$ for all p congruent to 2 modulo 3. Dodson [5] defined $\gamma^*(k, p^n)$ as the least positive integer t with the property that if $c_1, \dots, c_t$ are any integers coprime to p, then the congruence

$$c_1 x_1^k + \dots + c_t x_t^k \equiv 0 \bmod p^n$$

has a primitive solution, that is an integer solution with not all variables $x_1, \dots, x_t$ divisible by p. For $\delta = \gcd(k, p-1)$, he remarked that the non-zero residues modulo p form a cyclic group of order $p-1$ and hence, the sets $\left\{x^k : x \in \mathbb{F}_p\right\}$ and $\left\{x^\delta : x \in \mathbb{F}_p\right\}$ are equal, which implies $\gamma^*(k, p) = \gamma^*(\delta, p)$. Then he established the following connection between $\Gamma^*(k, p)$ and $\gamma^*(k, p^\gamma)$, where $p^\tau \parallel k$ and

$$\gamma = \begin{cases} \tau + 1, & \text{for } p > 2, \\ \tau + 2, & \text{for } p = 2. \end{cases}$$

LEMMA 3. *It holds* $\quad \Gamma^*(k, p) \leqslant k(\gamma^*(k, p^\gamma) - 1) + 1.$

Proof. See [5, Lemma 4.2.1]. □

For the cases $p \neq 2$ and $p \equiv 2 \bmod 3$, this provides

$$\Gamma^*(3, p) \leqslant 3\left(\gamma^*(3, p) - 1\right) + 1.$$

Here $\gamma^*(3, p) = \gamma^*(1, p)$ which is obviously 2 and hence $\Gamma^*(3, p) \leqslant 4$. The only remaining prime $p \equiv 2 \bmod 3$ is 2. Lemma 3 can be applied to show

$$\Gamma^*(3, 2) \leqslant 3\left(\gamma^*(3, 4) - 1\right) + 1.$$

It is easy to see that $\gamma^*(3, 4) = 2$ as well. If c_1, c_2 are coprime to 2, then they are congruent to 1 or 3 modulo 4. Since both 1 and -1 are cubic residues modulo 4, there is always a primitive solution of the equation

$$c_1 x_1^3 + c_2 x_2^3 \equiv 0 \bmod 4.$$

Hence, $\Gamma^*(3, 2) \leqslant 4$ as well and therefore, for all primes p congruent to 2 mod 3 Theorem 1 is fulfilled.

For primes congruent to 1 modulo 3, this does not give the desired result because $\Gamma^*(k, p)$ is too large. For them, I use a special case of Hensel's Lemma by Brüdern and Robert [2, Lemmata 4.1 and 4.2] to reduce the problem to one of congruences.

§3. *A special case of Hensel's lemma.* Throughout this section, I need the parameters τ and γ defined in the previous section which depend on the prime p and the degree of the first equation in the system (1.2). In Theorem 1, the degree is 3 and hence $\tau = 0$ for all $p > 3$ and $\tau = 1$ for $p = 3$ and $\gamma = \tau + 1$. The following lemma was proven by Brüdern and Robert [2, Lemma 4.2]. Although they excluded $k = 3$ before they proved it, the proof for $k = 3$ and $p > 2$ is the same.

LEMMA 4. *Let $s \geqslant 2$, $p > 2$ prime, and suppose that $\mathbf{x} \in \mathbb{Z}^s$ satisfies the congruences*

$$\sum_{j=1}^{s} a_j x_j^3 \equiv 0 \bmod p^{\gamma}, \quad \sum_{j=1}^{s} b_j x_j \equiv 0 \bmod p \tag{3.1}$$

and $p \nmid b_1 a_2 x_2^2 - b_2 a_1 x_1^2$. Then there are $y_1, y_2 \in \mathbb{Z}_p$ with $(y_1, y_2) \neq (0, 0)$ and

$$\sum_{j=1}^{s} a_j x_j^3 = \sum_{j=1}^{s} b_j x_j = 0.$$

For the remainder of this paper, a simultaneous solution of

$$\sum_{j=1}^{s} a_j x_j^3 \equiv 0 \bmod p^{\gamma} \quad \text{and} \quad \sum_{j=1}^{s} b_j x_j \equiv 0 \bmod p$$

is called non-singular if there are $1 \leqslant i, j \leqslant s$ such that $p \nmid b_i a_j x_j^2 - b_j a_i x_i^2$. The indices can be renumbered, if necessary, such that $p \nmid b_1 a_2 x_2^2 - b_2 a_1 x_1^2$. Then the preceding lemma can be applied to show that a non-singular solution implies a non-trivial p-adic one. This can be summarized to the following result.

LEMMA 5. *Let $s \geqslant 2$, $p > 2$ prime, γ defined as in the previous section and suppose*

$$\sum_{j=1}^{s} a_j x_j^3 \equiv 0 \bmod p^{\gamma}, \quad \sum_{j=1}^{s} b_j x_j \equiv 0 \bmod p \tag{3.2}$$

has a non-singular solution. Then (3.2) has a non-trivial p-adic one.

§4. *Conditioned systems.* In this section, I present conditioned systems, introduced by Brüdern and Robert [2] , which are a variant of the p-normalised systems of Davenport and Lewis [4]. One says that two systems (1.2) are equivalent if one can be converted into the other one by a finite series of the following processes.

(i) Substitute $(x_1, \ldots, x_s) \mapsto (c_1 x_1, \ldots, c_s x_s)$ with all $c_i \in \mathbb{Q}^{\times}$.
(ii) Multiplication of one of the equations by a non-zero rational number.
(iii) Permutation of indices.

If one representative of an equivalence class has a non-trivial p-adic solution, so has the whole class.

Brüdern and Robert [2, Section 6] showed that every system (1.2) with $a_i, b_i \in \mathbb{Q}\backslash\{0\}$ for $1 \leqslant i \leqslant s$ has an equivalent system with the properties that

(i) all coefficients a_i and b_i are non-zero integers;
(ii) there is an i with $p \nmid b_i$; and
(iii) the number of coefficients a_i with $p^j \nmid a_j$ is at least $\frac{js}{3}$ for $1 \leqslant j \leqslant 3$.

They called such a system conditioned. By combining this with a compactness argument, they have proven the following lemma.

LEMMA 6. *Suppose that for a fixed s there exists a non-trivial p-adic solution for all conditioned systems. Then all systems (1.2) with rational coefficients have non-trivial p-adic solutions.*

Proof. See [2, Lemma 6.1]. □

The work with conditioned systems and systems (1.2) requires the following notation.

(i) For $1 \leqslant i \leqslant s$, the parameters ν_i and μ_i are defined by $p^{\nu_i} \| a_i$ and $p^{\mu_i} \| b_i$.

(ii) The parameter t describes the number of $1 \leqslant i \leqslant s$ with $\nu_i = \mu_i = 0$.

(iii) For $j \in \mathbb{N}_0$, the parameter v_j is defined as the number of $1 \leqslant i \leqslant s$ such that $\nu_i = j$.

A variable x_i is called low if $\mu_i < \nu_i$ and high otherwise. The level of a variable x_i is defined by $\min(\mu_i, \nu_i)$. It follows from the definition of a conditioned system that $\nu_i \in \{0, 1, 2\}$, $v_0 \geqslant 3$, $v_0 + v_1 \geqslant 5$ and $v_0 + v_1 + v_2 = s$.

The set of systems

$$\sum_{j=1}^{s} a_j x_j^3 = \sum_{j=1}^{s} b_j x_j = 0 \tag{4.1}$$

with non-zero integers coefficients where $p^3 \nmid a_i$ $(1 \leqslant i \leqslant s)$ includes the set of conditioned systems. For each of the systems (4.1), there is an equivalent system in the same set with $\alpha_i p^{-\mu_i} b_i \equiv 1 \bmod p$, as one can find an $\alpha_i \in \mathbb{Z}$ such that $\alpha_i p^{-\mu_i} b_i \equiv 1 \bmod p$ for all $1 \leqslant i \leqslant s$, because $p^{\mu_i} \| b_i$. Applying $x_i \mapsto \alpha_i x_i$ for $1 \leqslant i \leqslant n$ provides such a system. As this transformation does not modify the parameters v_i and t, one can assume that every system (4.1), and hence, every conditioned system, has this property.

In the following, to prove that every conditioned system has a non-trivial solution, I will divide them into different sets, depending on the parameter used to describe them. To make the proofs that each of these sets has a non-trivial p-adic solution easier to follow, it is really helpful to establish an order of the variables in a conditioned system. A permutation of indices transforms a conditioned system into an equivalent one without changing the parameters v_i and t, while permutating the tuples (ν_i, μ_i) in the same manner as the indices. Therefore, to prove that every conditioned system with fixed parameters v_i $(0 \leqslant i \leqslant 2)$ and t has a non-trivial p-adic solution, it suffices to prove the existence of a non-trivial p-adic solution for every conditioned system with the same parameters having a fixed order of variables.

Definition 1. A system (4.1) is called an ordered system (4.1) if the variables with $\nu_i = 0$ are $x_1, \ldots, x_{v_0}$, whereas those with $\nu_i = 1$ are $x_{v_0+1}, \ldots, x_{v_0+v_1}$ and the remaining variables $x_{v_0+v_1+1}, \ldots, x_{v_0+v_1+v_2}$ are those with $\nu_i = 2$. Furthermore, the variables with $\nu_i = j$ for $j \in \{0, 1, 2\}$ are ordered, such that the ones with $p \nmid b_i$ are followed by those with $p \mid b_i$. If an ordered system (4.1) is also conditioned, it is called an ordered conditioned system.

As every system (1.2) is equivalent to an ordered conditioned system, it would suffice to prove the existence of a non-trivial p-adic solution for all ordered conditioned systems. In some cases, however, the proof also holds on a larger scale, hence some of the lemma will be slightly more general than others, which will prove to be useful.

§5. *The case* $p \equiv 1 \bmod 3$. As shown in § 3, one has to handle congruences modulo p, for which the following lemmata are useful tools.

LEMMA 7. *Let p be a prime, $\delta = (k, p-1)$, $p > 2\delta + 1$ and $\alpha_1, \dots, \alpha_n \not\equiv 0 \bmod p$. Then*

$$\alpha_1 x_1^k + \cdots + \alpha_n x_n^k \tag{5.1}$$

represent either all residues modulo p or at least $1 + ((2n-1)(p-1)/\delta)$.

Proof. See [3]. □

For $k = 3$ and primes congruent to 1 modulo 3, this implies $\delta = 3$, hence, for $p > 7$ this can be summed up as follows:

Conclusion 1. Let $p > 7$ be congruent to 1 modulo 3 and $\alpha_1, \alpha_2 \not\equiv 0 \bmod p$. Then $\alpha_1 x_1^3 + \alpha_2 x_2^3$ represent all residues modulo p. If additionally $\alpha_3 \not\equiv 0 \bmod p$, then

$$\alpha_1 x_1^3 + \alpha_2 x_2^3 + \alpha_3 x_3^3 \equiv 0 \bmod p$$

has a non-trivial solution with $x_1 \not\equiv 0 \bmod p$ arbitrary.

The following lemma provides a similar result for $p = 7$.

LEMMA 8. *Let $\alpha_1, \alpha_2, \alpha_3 \not\equiv 0 \bmod 7$. Then*

$$\alpha_1 x_1^3 + \alpha_2 x_2^3 + \alpha_3 x_3^3 \equiv 0 \bmod 7 \tag{5.2}$$

has a non-trivial solution.

Proof. For those $\alpha_i \equiv 4, 5$ or $6 \bmod 7$, one can apply $x_i \mapsto -x_i$ to transform (5.2) to an equation where all α_i are congruent to 1, 2 or 3 modulo 7. If now all coefficients are distinct modulo 7, it has, after a permutation of indices, if necessary, the form

$$x_1^3 + 2x_2^3 + 3x_3^3 \equiv 0 \bmod 7.$$

Setting $x_1 = x_2 = -x_3 = 1$, one obtains a non-trivial solution. Else there are $1 \leqslant i < j \leqslant 3$ with $\alpha_i \equiv \alpha_j \bmod 7$ and a non-trivial solution can be obtained by setting $x_i = -x_j = 1$ and the remaining variable 0. □

These lemmata can be used to provide a non-singular solution in a simple case.

LEMMA 9. *Let $p \equiv 1 \bmod 3$ be a prime, $a_1, a_2, a_3, b_4 \in \mathbb{F}_p^*$ and $b_1, b_2, b_3 \in \mathbb{F}_p$. Then there exists a non-singular solution in $\mathbb{F}_p$ of*

$$\sum_{i=1}^{3} a_i x_i^3 = \sum_{i=1}^{4} b_i x_i = 0.$$

Proof. Conclusion 1 and Lemma 8 provide a non-trivial solution of $\sum_{i=1}^{3} a_i x_i^3 = 0$ for all primes congruent to 1 modulo 3. After renumbering the indices, if necessary, one can assume that x_1 is not congruent to 0 modulo p. Setting x_4 such that $b_4 x_4 = -\sum_{j=1}^{3} b_j x_j$, this becomes a non-singular solution because $b_4 a_1 x_1^2 - b_1 a_4 x_4^2 \equiv b_4 a_1 x_1^2 \not\equiv 0 \bmod p$. □

This simple case can be applied to a lot of systems (4.1).

LEMMA 10. *Let $p \equiv 1 \bmod 3$ be a prime. An ordered system (4.1) with $v_0 \geqslant 3$ and a low variable at level 0 has a non-trivial p-adic solution.*

Proof. The variables $x_1, \dots, x_{v_0}$ are at level 0, but they are high. Therefore, there is a $j > v_0$ with $p \nmid b_j$. Set $x_i = 0$ for $i > 3$ and $i \neq j$. It remains to solve the system

$$\sum_{i=1}^{3} a_i x_i^3 \equiv \sum_{i=1}^{3} b_i x_i + b_j x_j \equiv 0 \bmod p,$$

for which Lemma 9 provides a non-singular solution. Hence, Lemma 5 can be used to lift the non-singular solution to a non-trivial p-adic one. □

LEMMA 11. *Let* $p \equiv 1 \bmod 3$ *be a prime. Suppose* $v_j \geqslant 3$ *for* $j \in \{1, 2\}$. *Then an ordered conditioned system has a non-trivial p-adic solution if* $s \geqslant 8$.

Proof. An ordered conditioned system with $s \geqslant 8$ has by definition $v_0 \geqslant 3$ and hence, if it has a low variable at level 0, the existence of a non-trivial p-adic solution follows from Lemma 10.

In an ordered conditioned system without a low variable at level 0, the coefficients b_i $(v_0 < i \leqslant s)$ are divisible by p, hence, $p \nmid b_1$. Writing $\mathbf{x}_0 = (x_1, \dots, x_{v_0})$, $\mathbf{x}_1 = (x_{v_0+1}, \dots, x_{v_0+v_1})$ and $\mathbf{x}_2 = (x_{v_0+v_1+1}, \dots, x_s)$ the cubic term can be seen as

$$\sum_{i=1}^{s} a_i x_i^3 = f_0(\mathbf{x}_0) + p f_1(\mathbf{x}_1) + p^2 f_2(\mathbf{x}_2), \tag{5.3}$$

where $f_j(\mathbf{x}_j) = p^{-j} \sum_{v_i = j} a_i x_i^3$ are polynomials in $\mathbb{Z}[x_1, \dots, x_s]$. Apply $x_i \mapsto p x_i$ for $1 \leqslant i \leqslant v_0$ or $1 \leqslant i \leqslant v_0 + v_1$ if $j = 1$ or $j = 2$, respectively, and divide the cubic equation by p^j and the linear one by p. This provides an equivalent system (4.1) and changes (5.3) into

$$\begin{cases} p^2 f_0(\mathbf{x}_0) + f_1(\mathbf{x}_1) + p f_2(\mathbf{x}_2), & \text{for } j = 1 \\ p f_0(\mathbf{x}_0) + p^2 f_1(\mathbf{x}_1) + f_2(\mathbf{x}_2), & \text{for } j = 2. \end{cases}$$

The altered cubic term has at least three variables with $p \nmid a_i$. Furthermore $p \mid a_{i_0}$ and $p \nmid b_{i_0}$, hence $v_0 \geqslant 3$ and it exists a low variable at level 0. By applying a permutation of indices, one obtains an ordered system (4.1), hence, all conditions of Lemma 10 are fulfilled and a non-trivial p-adic solution exists. □

The impact of the two previous lemmata can be summarised as follows.

LEMMA 12. *If an ordered conditioned system with* $s \geqslant 8$ *does not have a non-trivial p-adic solution for all primes p congruent to* 1 *modulo* 3, *then*

$$v_0 \geqslant 4, \qquad v_1 \leqslant 2, \qquad v_2 \leqslant 2$$

and there exists no low variable at level zero.

Proof. It follows from Lemma 11 that v_1 and v_2 have to be at most 2. But since $s \geqslant 8$ it follows that $v_0 \geqslant 4$. Furthermore, Lemma 10 can be applied to show that no low variable at level zero exists. □

To prove Theorem 1 for all primes congruent to 1 modulo 3, it remains to show the existence of a non-trivial p-adic solution for those conditioned systems (4.1) described in Lemma 12, which can be divided up into different sets, depending on the correlation between v_0 and t.

LEMMA 13. *An ordered conditioned system has a non-trivial p-adic solution provided* $v_0 \geqslant t+3$ *and* $p \equiv 1 \bmod 3$ *is a prime.*

Proof. Set $x_i = 0$ for all $1 \leqslant i \leqslant t$ and $t+4 \leqslant i \leqslant s$. Hence, all x_i with $p \nmid b_i$ are 0. This ensures that the linear equation is congruent to 0 modulo p independently of the choice of the remaining variables. Then, Conclusion 1 and Lemma 8 provide a non-trivial solution of the cubic equation

$$a_{t+1}x_{t+1}^3 + a_{t+2}x_{t+2}^3 + a_{t+3}x_{t+3}^3 \equiv 0 \bmod p,$$

with $x_{t+j} \not\equiv 0 \mod p$ for some $j \in \{1, 2, 3\}$. A conditioned system has, by definition, an x_i with $p \nmid b_i$, which was set 0 at the beginning of this proof. Hence, this is a non-singular solution of the ordered conditioned system, because $b_i a_{t+j} x_{t+j}^2 - b_{t+j} a_i x_i^2 \equiv b_i a_{t+j} x_{t+j}^2 \not\equiv 0 \bmod p$, which can be lifted to a non-trivial p-adic solution with Lemma 5. □

LEMMA 14. *Let* $3 \leqslant m \leqslant n$ *and* $a_i \not\equiv 0 \mod p$ *for* $1 \leqslant i \leqslant n$. *If there are* $1 \leqslant i < j \leqslant m$ *such that* $a_i \equiv a_j \bmod p$, *then*

$$\begin{aligned} a_1x_1^3 + \cdots + a_mx_m^3 + a_{m+1}x_{m+1}^3 + \cdots + a_nx_n^3 &\equiv 0 \bmod p, \\ x_1 + \cdots + x_m \qquad\qquad\qquad\qquad &\equiv 0 \bmod p \end{aligned}$$

has a non-singular solution.

Proof. Set $x_i = -x_j = 1$ and the remaining variables 0. This solves the equations non-singular because

$$\begin{aligned} a_1x_1^3 + \cdots + a_nx_n^3 &\equiv a_ix_i^3 + a_jx_j^3 \equiv a_i - a_j \equiv 0 \bmod p, \\ x_1 + \cdots + x_m &\equiv x_i + x_j \qquad \equiv 1 - 1 \quad \equiv 0 \bmod p, \end{aligned}$$

and there is a $k \neq i, j$ with $1 \leqslant k \leqslant m$, for which x_k has the value 0 and $a_k x_k^2 b_i - a_i x_i^2 b_k \equiv -a_i \not\equiv 0 \bmod p$. □

This allows to handle the cases $v_0 = t+2 \geqslant 5$ and $v_0 = t+1 \geqslant 5$, as will be done in the next two lemmata.

LEMMA 15. *Let* $p \equiv 1 \bmod 3$ *be a prime. An ordered conditioned system with* $v_0 = t+2 \geqslant 5$ *has a non-trivial p-adic solution.*

Proof. If $a_1 \equiv a_2 \mod p$, then Lemma 14 provides a non-singular solution as $t \geqslant 3$. If they are distinct modulo p, setting all variables 0, except x_1, x_2, x_{t+1} and x_{t+2}, the system transforms to

$$\begin{aligned} a_1x_1^2 + a_2x_2^3 + a_{t+1}x_{t+1}^3 + a_{t+2}x_{t+2}^3 &\equiv 0 \bmod p, \\ x_1 + \quad x_2 \qquad\qquad\qquad &\equiv 0 \bmod p. \end{aligned}$$

The linear equation can be solved by setting $x_1 = -x_2 = x$ without giving an explicit value to x. All that remains of the cubic equation is

$$(a_1 - a_2)x^3 + a_{t+1}x_{t+1}^3 + a_{t+2}x_{t+2}^3 \equiv 0 \bmod p.$$

Conclusion 1 and Lemma 8 provide a non-trivial solution because $a_1 - a_2 \not\equiv 0 \bmod p$, hence, there is an $i \in \{1, t+1, t+2\}$ with $x_i \not\equiv 0 \bmod p$. Because $a_i x_i^2 b_3 - b_i a_3 x_3^2 \equiv b_3 a_i x_i^2 \not\equiv$

$0 \bmod p$, both cases have a non-singular solution and Lemma 5 provides the required non-trivial p-adic solution. □

LEMMA 16. *Let $p \equiv 1 \bmod 3$ be a prime. An ordered conditioned system with $v_0 = t + 1 \geqslant 5$ has a non-trivial p-adic solution.*

Proof. Set all variables 0 except $x_1, \dots, x_4$ and x_{v_0}. The obtained system has the form

$$\begin{aligned} a_1x_1^3 + \cdots + a_4x_4^3 + a_{v_0}x_{v_0}^3 &\equiv 0 \bmod p, \\ x_1 + \cdots + \quad x_4 \qquad\qquad &\equiv 0 \bmod p. \end{aligned}$$

If two of the coefficients $a_1, \dots, a_4$ are equivalent modulo p, Lemma 14 provides a non-singular solution. Else, one can assume that all a_i modulo p are distinct for $1 \leqslant i \leqslant 4$. Set $x_1 = -x_2 = y_1$ and $x_3 = -x_4 = y_2$. It follows that

$$\begin{aligned} a_1x_1^3 + \cdots + a_4x_4^3 + a_{v_0}x_{v_0}^3 &\equiv (a_1 - a_2)y_1^3 + (a_3 - a_4)y_2^3 + a_{v_0}x_{v_0}^3 \bmod p, \\ x_1 + \cdots + \quad x_4 \qquad\qquad &\equiv y_1 - y_1 + y_2 - y_2 \equiv 0 \bmod p. \end{aligned}$$

As both $a_1 - a_2$ and $a_3 - a_4$ are not congruent to 0 modulo p, Conclusion 1 and Lemma 8 provide y_1, y_2 and x_{v_0} which are not all divisible by p, such that the cubic equation is fulfilled. If not all three are divisible by p, then at least two of them are not, and hence, one of y_1 and y_2, say y_j, is not divisible by p. It follows that $b_{2j}a_{2j-1}x_{2j-1}^2 - b_{2j-1}a_{2j}x_{2j}^2 \equiv a_{2j-1}y_j^2 - a_{2j}y_j^2 \equiv (a_{2j-1} - a_{2j})y_j^2 \not\equiv 0 \bmod p$ and therefore Lemma 5 provides a non-trivial p-adic solution for both cases. □

The following lemma uses that the non-zero cubics modulo p are a multiplicative group with $\frac{p-1}{3}$ elements, hence, $\mathbb{F}_p^*$ is the disjunct union of $\left(\mathbb{F}_p^*\right)^3$ and its two cosets and every element in one of the three cosets can be transformed in one of the same coset by multiplying it with a cube.

LEMMA 17. *Let $p \equiv 1 \bmod 3$ be a prime. An ordered conditioned system with $t \geqslant 5$ has a non-trivial p-adic solution.*

Proof. If $a_1, \dots, a_5$ are not distinct modulo p, Lemma 14 provides a non-singular solution. Else, if they are distinct modulo p, at least two of them have to be in the same coset of $\left(\mathbb{F}_p^*\right)^3$. After a permutation of the first five indices, one can assume that these are a_1 and a_2. Hence, there is a $b \in \mathbb{Z}$ not congruent to 0 or 1 modulo p such that $b^3a_1 \equiv a_2 \bmod p$. Put $x_1 = by$, $x_2 = -y$ and $x_i = 0$ for all $i \geqslant 6$. This transforms the cubic equation of the system into

$$\begin{aligned} a_1x_1^3 + a_2x_2^3 + a_3x_3^3 + a_4x_4^3 + a_5x_5^3 &\equiv a_1b^3y^3 - a_2y^3 + a_3x_3^3 + a_4x_4^3 + a_5x_5^3 \\ &\equiv a_1b^3y^3 - a_1b^3y^3 + a_3x_3^3 + a_4x_4^3 + a_5x_5^3 \\ &\equiv a_3x_3^3 + a_4x_4^3 + a_5x_5^3 \bmod p \end{aligned}$$

and the linear equation into

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 + x_5 &\equiv by - y + x_3 + x_4 + x_5 \\ &\equiv (b-1)y + x_3 + x_4 + x_5 \bmod p. \end{aligned}$$

Conclusion 1 and Lemma 8 provide a non-trivial solution of the cubic equation with an $i \in \{3, 4, 5\}$ such that $x_i \not\equiv 0 \mod p$. As $b - 1 \not\equiv 0 \mod p$, it is possible to choose y in a way that the linear equation is simultaneously fulfilled.

To show that the obtained solution is non-singular, one has to separate the case $y \equiv 0 \mod p$. If $y \not\equiv 0 \mod p$, then $b_2a_1x_1^2 - b_1a_2x_2^2 \equiv a_1b^2y^2 - a_1b^3y^2 \equiv a_1b^2y^2(1 - b) \not\equiv 0 \mod p$, else, $y \equiv 0 \mod p$ and $b_1a_ix_i^2 - b_ia_1x_1^2 \equiv a_ix_i^2 - a_1b^2y^2 \equiv a_ix_i^2 \not\equiv 0 \mod p$. This has proven that there exist a non-singular solution, which can be lifted to a non-trivial p-adic one by Lemma 5. □

The cases not yet proven are those with $(v_0, t) \in \{(4, 2), (4, 3), (4, 4)\}$. These cases are more complex than the previous one, hence, I am going to treat them in the following two chapters.

§6. *The case* $(v_0, t) = (4, 2)$. The main part of this case can be handled as the cases in the previous section, with the prime $p = 7$ being treated individually.

LEMMA 18. *Let* $p \equiv 1 \mod 3$ *be a prime with* $p > 7$*. An ordered conditioned system with* $v_0 = 4$*,* $t = 2$ *and* $a_1 \not\equiv a_2 \mod p$ *has a non-trivial* p*-adic solution.*

Proof. Setting $x_1 = 1, x_2 = -1$ and $x_i = 0$ for $i \geqslant 5$ solves the linear equation. The cubic equation transforms to $a_1 - a_2 + a_3x_3^3 + a_4x_4^3 \equiv 0 \mod p$, which has, due to Conclusion 1, a solution which is non-singular as $a_1x_1^2b_2 - a_2x_2^2b_1 \equiv a_1 - a_2 \not\equiv 0 \mod p$ and can be lifted with Lemma 5. □

LEMMA 19. *An ordered conditioned system with* $v_0 = 4$ *and* $t = 2$*, where* $a_1 \not\equiv a_2 \mod 7$*, has a non-trivial* 7*-adic solution.*

Proof. A multiplication of the cubic equation with α such that $\alpha a_3 \equiv 1 \mod 7$ still leaves $a_1 \not\equiv a_2 \mod 7$. So does the application of $x_4 \mapsto -x_4$, if necessary, to ensure that a_4 is congruent to either 1, 2 or 3 modulo 7. If $a_4 \equiv 1 \mod 7$, set $x_3 = 1, x_4 = -1$ and everything else 0. This solves the cubic and the linear equation modulo 7 and because $a_3x_3^2b_1 - a_1x_1^2b_3 \equiv a_3 \equiv 1 \mod 7$ this solution is non-singular. The cases with $a_4 \equiv 2, 3 \mod 7$ can be solved by choosing $x_3, x_4 \in \{-1, 0, 1\}$, not both 0, such that $a_3x_3^3 + a_4x_4^3 \equiv \pm(a_1 - a_2) \mod 7$ and then setting $x_1 = \mp 1$ and $x_2 = \pm 1$, such that the cubic solution is solved as well modulo 7. Let $i \in \{3, 4\}$ be such that $x_i \not\equiv 0 \mod 7$. Then $a_ix_i^2b_1 - a_1x_1^2b_i \equiv a_i \not\equiv 0 \mod 7$. Both times the solution can be lifted with Lemma 5. □

It remains the ordered conditioned systems where $a_1 \equiv a_2 \mod p$. Multiplying the cubic equation with $b_1^3b_2^3$ and applying $b_1x_1 \mapsto x_1$ and $b_2x_2 \mapsto x_2$ do not change the values of ν_j and μ_j because $b_1^3b_2^3 \equiv 1 \mod p$ and the characteristic $a_1 \equiv a_2 \mod p$ stays untouched as well, because $b_1 \equiv b_2 \equiv 1 \mod p$. This transforms the ordered conditioned system in an equivalent ordered conditioned system with coefficients a_i and b_i with $b_1 = b_2 = 1$. By choosing an integer α with $a_1\alpha \equiv 1 \mod p$ and multiplying the cubic equation with it, one gets $a_1 \equiv a_2 \equiv 1 \mod p$. Furthermore, one can assume that $a_1 \neq a_2$ because else, setting $x_1 = 1, x_2 = -1$ and the remaining variables 0 solves the system. Therefore, there is a $\theta \in \mathbb{N}$ such that $a_1 - a_2 = p^\theta a'$.

The last two lemmata gave useful information about the coefficients of the first two variables, whereas the following lemma will give some additional information about the coefficients of the remaining coefficients of the cubic equation, for which further notation is needed.

Definition 2. Two integers a and b differ by a cube, say $[a] = [b]$, if there is a $c \not\equiv 0 \bmod p$ such that $a \equiv c^3 b \bmod p$.

LEMMA 20. *If an ordered conditioned system with $a_1 \equiv a_2 \equiv 1 \bmod p$, $b_1 = b_2 = 1$, $v_0 = 4$, $v_1 = 2$, $v_2 = 2$ and $t = 2$, which has no low variable at level 0, has no non-trivial p-adic solution for a prime $p \equiv 1 \bmod 3$, then for all $i \in \{0, 1, 2\}$ it has to hold that*

$$[a_{2i+3}] \neq [a_{2i+4}].$$

Proof. Assume that there is an $i \in \{0, 1, 2\}$ such that $a_{2i+3} \equiv c^3 a_{2i+4}$. Set all variables 0 except x_1, x_{2i+3} and x_{2i+4} and apply $x_1 \mapsto p x_1$. Dividing the cubic equation by p^i and the linear by p transforms the system into one with $\nu_1 = 3 - i \geqslant 1$, $\nu_{2i+3} = \nu_{2i+4} = 0$, $\mu_1 = 0$ and $\mu_{2i+3}, \mu_{2i+4} \geqslant 0$. Setting $x_{2i+3} = 1$ and $x_{2i+4} = -c$ solves the cubic equation independent of the values of x_1 modulo p. Taking x_1 such that the linear equation is solved modulo p provides a solution, which can be lifted, because of $a_1 x_1^2 b_{2i+3} - a_{2i+3} x_{2i+3}^2 b_1 \equiv -a_{2i+3} \not\equiv 0 \bmod p$, with Lemma 5. □

Definition 3. An ordered conditioned system with $a_1 \equiv a_2 \equiv 1 \bmod p$, $b_1 = b_2 = 1$, $v_0 = 4$, $v_1 = 2$, $v_2 = 2$, $t = 2$ and $\theta \in \mathbb{N}$ such that $a_1 - a_2 = p^\theta a'$ which has no low variable at level 0 is called a critical system if $[a_{2i+3}] \neq [a_{2i+4}]$ for all $i \in \{0, 1, 2\}$.

To conclude the case $v_0 = 4$ and $t = 2$, I will have to prove that every critical system has a non-trivial p-adic solution for all primes $p \equiv 1 \bmod 3$. To handle them, I am going to prove some lemmata, starting with one, similar to Lemma 8, fitting better for critical systems and proceeding with a tool which uses the knowledge about a_1 and a_2.

LEMMA 21. *Let $a' c_1 c_2 \not\equiv 0 \bmod 7$ and $[c_1] \neq [c_2]$. Then $a' + c_1 y_1^3 + c_2 y_2^3 \equiv 0 \bmod 7$ has a non-trivial solution.*

Proof. Without loss of generality, I can assume that $a' \equiv 1 \bmod 7$. Else, multiplying the equation with a $b \in \mathbb{Z}$ such that $a'b \equiv 1 \bmod 7$ turns it into such an equation. If there is an $i \in \{1, 2\}$ such that $c_i \equiv \pm 1 \bmod 7$ set $x_i = \mp 1$ and the other variable 0. Else, $c_i \in \{\pm 2, \pm 3\}$, but $[c_1] \neq [c_2]$, hence there are $i, j \in \{1, 2\}$ with $c_i \in \{\pm 2\}$ and $c_j \in \{\pm 3\}$. Choose $x_i \in \{\pm 1\}$ such that $c_i x_i^3 \equiv 2 \bmod 7$ and $x_j \in \{\pm 1\}$ such that $c_j x_j^3 \equiv -3 \bmod 7$. This solves the equation non-trivially. □

LEMMA 22. *Let $p \equiv 1 \bmod 3$, $a_1 - a_2 = p^\theta a'$ for some $\theta \in \mathbb{N}$ and $a_1 \equiv a_2 \equiv 1 \bmod p$. Let c and d be integers with $p \nmid cd$ and $\left(\frac{cd}{p}\right) = \left(\frac{3}{p}\right)$. Then, for each l with $1 \leqslant l < \theta$, there are integers x_1, x_2 and c' with $c' \equiv c \bmod p$, $a_1 x_1^3 + a_2 x_2^3 = p^l c'$ and $x_1 + x_2 = p^l d$.*

Proof. Set $x_1 = x + p^l d$ and $x_2 = -x$. Choose x such that $3 a_1 x^2 d \equiv c \bmod p$. This is possible because

$$\left(\frac{3^{-1} a_1^{-1} d^{-1} c}{p}\right) = \left(\frac{3 a_1 c d}{p}\right) = \left(\frac{3}{p}\right)^2 = 1.$$

This gives

$$\begin{aligned} a_1x_1^3 + a_2x_2^3 &= a_1x^3 + 3a_1x^2dp^l + 3a_1xd^2p^{2l} + a_1d^3p^{3l} - a_2x^3 \\ &= p^\theta a'x^3 + 3a_1x^2dp^l + 3a_1xd^2p^{2l} + a_1d^3p^{3l} \\ &\equiv 3a_1x^2dp^l \equiv cp^l \bmod p^{l+1}, \end{aligned}$$

and hence, $a_1x_1^3 + a_2x_2^3 = c'p^l$ for some $c' \equiv c \bmod p$. □

LEMMA 23. *Let $p \equiv 1 \bmod 3$, $a_1 - a_2 = p^\theta a'$, $a_1 \equiv a_2 \equiv 1 \bmod p$, $c_1, c_2, d_1, d_2, e, f \in \mathbb{Z}$ such that $p \nmid c_1c_2f$, $[c_1] \neq [c_2]$ and $1 \leqslant \beta < \theta$. Then the system of equation*

$$a_1x_1^3 + a_2x_2^3 + p^\beta\left(c_1y_1^3 + c_2y_2^3\right) + p^{\beta+1}ez^3 = 0,$$

$$x_1 + x_2 + p^\beta\left(d_1y_1 + d_2y_2\right) + p^\beta fz = 0$$

has a non-trivial solution $(x_1, x_2, y_1, y_2, z) \in \mathbb{Q}_p^5$.

Proof. As $[c_1] \neq [c_2]$, it follows that $c_1 \not\equiv -c_2 \bmod p$. Hence, $-c_1 - c_2 \not\equiv 0 \bmod p$ and therefore, one can apply Lemma 22 with $l = \beta$ and $c = -c_1 - c_2$ while choosing $d \in \{\pm 1\}$ such that $\left(\frac{cd}{p}\right) = \left(\frac{3}{p}\right)$. This provides x_1, x_2 and $c' \equiv c \bmod p$ such that

$$a_1x_1^3 + a_2x_2^3 + p^\beta\left(c_1y_1^3 + c_2y_2^3\right) + p^{\beta+1}ez^3 = p^\beta c' + p^\beta\left(c_1y_1^3 + c_2y_2^3\right) + p^{\beta+1}ez^3$$

and

$$x_1 + x_2 + p^\beta\left(d_1y_1 + d_2y_2\right) + p^\beta fz = p^\beta d + p^\beta\left(d_1y_1 + d_2y_2\right) + p^\beta fz.$$

Dividing both equation by p^β and setting $y_1 = y_2 = 1$ leave the system

$$c' + c_1 + c_2 + pez^3 = 0,$$

$$d + d_1 + d_2 + fz = 0$$

to be solved. As c' solves the upper equation modulo p, choosing z so that the lower equation is solved modulo p gives a solution of the system modulo p. Since $c_1y_1^2f - pez^2d_1 \equiv c_1f \not\equiv 0 \bmod p$, this solution can be lifted with Lemma 5 to a solution in $\mathbb{Q}_p^5$ of the system. □

LEMMA 24. *A critical system with a low variable at level $\beta < \theta$ has a non-trivial p-adic solution.*

Proof. Choose a low variable x_t with level β smallest among the low variables of the system. Critical systems have no low variables at level 0, hence, $1 \leqslant \beta \leqslant \theta - 1$. Due to the minimality of β, the variables $x_{2\beta+3}$ and $x_{2\beta+4}$ are high variables at level β. Put all variables 0, except $x_1, x_2, x_{2\beta+3}, x_{2\beta+4}$ and x_t. This is a system as in Lemma 23, hence, it has a non-trivial p-adic solution. □

LEMMA 25. *Let $p \equiv 1 \bmod 3$, $a_1 - a_2 = p^\theta a'$, $a_1 \equiv a_2 \equiv 1 \bmod p$, $c_1, c_2, d_1, d_2 \in \mathbb{Z}$ such that $p \nmid c_1c_2d_1$, $d_1 \equiv 1 \bmod p$ and d_2 is congruent to either 0 or 1 modulo p, $c_1 \not\equiv c_2 \bmod p$ and $1 \leqslant \beta \leqslant \theta - 3$. Then the system of equations*

$$a_1x_1^3 + a_2x_2^3 + p^\beta\left(c_1y_1^3 + c_2y_2^3\right) = 0,$$

$$x_1 + x_2 + p^\beta\left(d_1y_1 + d_2y_2\right) = 0$$

has a non-trivial p-adic solution.

Proof. Set $y_1 = y_1' p$, $y_2 = y_2' p$, $x_1 = 1 + dp^{\beta+3}$ and $x_2 = -1$. This provides the system of equation

$$a' p^{\theta} + 3da_1 p^{\beta+3} + 3d^2 a_1 p^{2\beta+6} + a_1 d^3 p^{3\beta+9} + p^{\beta+3}\left(c_1 y_1'^3 + c_2 y_2'^3\right) = 0,$$
$$dp^{\beta+3} + p^{\beta+1}\left(d_1 y_1' + d_2 y_2'\right) = 0,$$

where the upper equation can be divides by $p^{\beta+3}$ and the lower by $p^{\beta+1}$. In the case $d_2 \equiv 0 \bmod p$, this transforms, modulo p, into

$$a' p^{\theta-\beta-3} + 3d + c_1 y_1'^3 + c_2 y_2'^3 \equiv 0 \bmod p,$$
$$y_1' \equiv 0 \bmod p.$$

Setting $y_1' = 0$, $y_2' = 1$, and choosing d such that $3d \equiv -c_2 - a' p^{\theta-\beta-3} \bmod p$ give a non-singular solution, because of $c_1 y_1'^2 d_2 - c_2 y_2'^2 d_1 \equiv -c_2 \not\equiv 0 \bmod p$. In the case $d_2 \equiv 1 \bmod p$, this transforms the system, modulo p, into

$$a' p^{\theta-\beta-3} + 3d + c_1 y_1'^3 + c_2 y_2'^3 \equiv 0 \bmod p,$$
$$y_1' + y_2' \equiv 0 \bmod p.$$

Setting $y_1' = 1$, $y_2' = -1$ and d such that $3d \equiv -c_1 + c_2 - a' p^{\theta-\beta-3} \bmod p$ gives a non-singular solution because of $c_1 y_1'^2 d_2 - c_2 y_2'^2 d_1 \equiv c_1 - c_2 \not\equiv 0 \bmod p$. In both cases, the solution can be lifted with Lemma 5. □

The following lemma concerning the number of zeros of an absolute irreducible polynomial $f(x, y)$ with coefficients in $\mathbb{F}_q$ will prove useful in the remaining steps.

LEMMA 26. *An absolutely irreducible polynomial $f(x, y)$ with coefficients in $\mathbb{F}_q$ of degree $d > 0$ has*

$$N \geqslant q + 1 - \frac{1}{2}(d-1)(d-2)\left[2q^{\frac{1}{2}}\right] - d$$

where N is the number of zeros of $f(x, y)$.

Proof. See [6, Corollary 2.b]. □

In the following, $\deg_x(k(x, y))$ and $\deg_y(k(x, y))$ will denote the degree in x and y, respectively, of a polynomial $k(x, y)$.

LEMMA 27. *The polynomial $f(x, y) = a'x^3 - 3yx^2 + c_1 y^3 + c_2 \in \mathbb{F}_p[x, y]$ has a zero for all $p \equiv 1 \bmod 3$ if $a'c_1c_2 \not\equiv 0 \bmod p$.*

Proof. Assuming that $f(x, y)$ is reducible in $\overline{\mathbb{F}}_p$, there are polynomials $g(x, y), h(x, y) \in \overline{\mathbb{F}}_p[x, y]$ such that $f(x, y) = g(x, y) \cdot h(x, y)$. Without loss of generality, one can assume that $\deg_x(g(x, y)) \geqslant \deg_x(h(x, y))$, hence, $\deg_x(g(x, y)) = 2$ and $\deg_x(h(x, y)) = 1$. Writing

$$g(x, y) = g_2(y)x^2 + g_1(y)x + g_0 \qquad \text{and} \qquad h(x, y) = h_1(y)x + h_0(y)$$

with $g_i(y), h_j(y) \in \overline{\mathbb{F}}_p[y]$ for $0 \leqslant i \leqslant 2$ and $0 \leqslant j \leqslant 1$, one obtains $\deg_y(g_2(y)) = \deg_y(h_1(y)) = 0$, $\deg_y(g_1(y)) = \deg_y(h_0(y)) = 1$ and $\deg_y(g_0(y)) = 2$ by comparing the degree of the polynomial in y in front of x^i in $f(x, y)$ with that in $g(x, y) \cdot h(x, y)$. Therefore, one can write the polynomials $g_i(y)$ and $h_i(y)$ as

$$g_0(y) = g_{02}y^2 + g_{01}y + g_{00}, \qquad g_1(y) = g_{11}y + g_{10}, \qquad g_2(y) = g_{20},$$
$$h_0(y) = h_{01}y + h_{00}, \qquad h_1(y) = h_{10}$$

with $g_{ij}, h_{ij} \in \overline{\mathbb{F}}_p$, where $g_{02}g_{11}g_{20}h_{01}h_{10} \neq 0$. By dividing $h(x, y)$ by h_{10} and multiplying $g(x, y)$ with it, one can assume that $h_{10} = 1$. A comparison of the polynomials in y in front of x^3 of both sides of $f(x, y) = g(x, y) \cdot h(x, y)$ shows $g_{20} = a'$. Likewise, the polynomials in y in front of x^0 leads to the equations

$$g_{02}h_{01} = c_1, \tag{6.1}$$

$$g_{01}h_{01} = -g_{02}h_{00}, \tag{6.2}$$

$$g_{01}h_{00} = -g_{00}h_{01}, \tag{6.3}$$

$$g_{00}h_{00} = c_2. \tag{6.4}$$

From (6.4), it follows that $g_{00}h_{00} \neq 0$ and hence, (6.1) and (6.4) provide

$$h_{01} = \frac{c_1}{g_{02}} \quad \text{and} \quad h_{00} = \frac{c_2}{g_{00}},$$

which can be inserted into (6.2) to obtain

$$g_{01} = -\frac{c_2}{c_1}\frac{g_{02}^2}{g_{00}}.$$

Inserting all of this in (6.3) leads to

$$c_2^2 g_{02}^3 = c_1^2 g_{00}^3. \tag{6.5}$$

The equation $g_{20}h_{00} + g_{10}h_{10} = 0$ can be obtained by comparing the polynomial in y in front of x^2. Using what was already obtained before, one gets

$$g_{10} = -\frac{c_2 a'}{g_{00}}.$$

The polynomial in y in front of x provides the equations

$$g_{11}h_{01} + g_{02}h_{10} = 0, \qquad g_{11}h_{00} + g_{10}h_{01} + g_{01}h_{10} = 0, \qquad g_{10}h_{00} + g_{00}h_{10} = 0,$$

which, combined with the established equations, shows

$$2g_{02}^3 = -c_1^2 a', \tag{6.6}$$

$$c_2^2 a' = g_{00}^3. \tag{6.7}$$

By inserting (6.7) into (6.5), it follows $g_{02}^3 = c_1^2 a'$ which, together with (6.6), leads to $-c_1^2 a' = 2g_{02}^3 = 2c_1^2 a'$. It would follow that $-1 = 2$, which is false, because $p > 3$, and hence, such a factorisation cannot exist and $f(x, y)$ is absolute irreducible. The total degree of $f(x, y)$ is 3, and therefore, for N being the number of zeros of $f(x, y)$ in $\mathbb{F}_p$, Lemma 26 shows

$$N \geqslant p - \left[2\sqrt{p}\right] - 2.$$

For $p > 7$, it follows that there is a zero of $f(x, y)$. The only prime $p \leqslant 7$ with $p \equiv 1 \bmod 3$ is seven. It is possible to find a solution for all values of a', c_1 and c_2 where $a'c_1c_2 \not\equiv 0 \bmod 7$ holds as described in the following. The equation

$$dx^3 + c_2 \equiv 0 \bmod p \tag{6.8}$$

is solvable, if $[d] = [c_2]$, because then, there is a $b \in \mathbb{F}_p$ such that $db^3 \equiv c_2 \bmod p$ and hence, $x \equiv -b \bmod p$ is a solution. Setting $x = 0$ or $y = tx$ with $t \in \mathbb{F}_7$ in $f(x, y)$, one obtains an equation of this type; with various values for d, in fact, it can be c_1, a', $a' + c_1 + i$ and $a' - c_1 + j$ with $i \in \{1, 2, 4\}$ and $j \in \{3, 5, 6\}$. In the following, one sees that for every value of (a', c_1, c_2), for at least one of the possible values of d it holds $[d] = [c_2]$ and hence, there is always a solution.

In $\mathbb{F}_7$, it holds $[1] = [6]$, $[2] = [5]$ and $[3] = [4]$. Assume (a', c_1, c_2) are such that $f(x, y)$ has no zero. For $d = c_1$, it follows that $[c_1] \neq [c_2]$ and from $d = a'$ that $[a'] \neq [c_2]$. If $a' \equiv -c_1 \bmod 7$ or $a' \equiv c_1 \bmod 7$, the values $d = a' + c_1 + i$ with $i \in \{1, 2, 4\}$ or $d = a' - c_1 + i$ with $i \in \{3, 5, 6\}$, respectively, represents each equivalence class and it is always possible to choose x and y such that $[d] = [c_2]$. But then, $f(x.y)$ would have a zero, hence $[a'] \neq [c_1]$. If a' is chosen, it follows that c_1 can only be in one of the two remaining equivalence classes, and if c_1 is chosen as well, the equivalence class of c_2 is fixed. In the following table all possible values of (a', c_1) with $[a'] \neq [c_1]$ are listed together with a value for d which is in the remaining equivalence class, showing that there is no possible value for c_2 such that there is no zero of $f(x, y)$, which proves the Lemma.

a'	c_1	d	a'	c_1	d	a'	c_1	d	a'	c_1	d
1	2	$a' + c_1 + 1$	2	4	$a' + c_1 + 2$	4	1	$a' + c_1 + 4$	5	4	$a' + c_1 + 4$
1	3	$a' + c_1 + 1$	2	6	$a' + c_1 + 2$	4	2	$a' + c_1 + 2$	5	6	$a' - c_1 + 5$
1	4	$a' - c_1 + 5$	3	1	$a' + c_1 + 1$	4	5	$a' + c_1 + 4$	6	2	$a' + c_1 + 2$
1	5	$a' + c_1 + 4$	3	2	$a' + c_1 + 1$	4	6	$a' + c_1 + 2$	6	3	$a' - c_1 + 6$
2	1	$a' + c_1 + 1$	3	5	$a' - c_1 + 3$	5	1	$a' + c_1 + 4$	6	4	$a' - c_1 + 3$
2	3	$a' + c_1 + 1$	3	6	$a' - c_1 + 5$	5	3	$a' - c_1 + 6$	6	5	$a' - c_1 + 3$

□

LEMMA 28. *The polynomial* $f(x, y) = c_1x^3 - 3x + c_2y^3 - 3y + a' \in \mathbb{F}_p[x, y]$ *is absolute irreducible for all primes* $p \equiv 1 \bmod 3$.

Proof. Assuming that $f(x, y)$ is reducible in $\overline{\mathbb{F}}_p[x, y]$, there exists polynomials $g(x, y), h(x, y) \in \overline{\mathbb{F}}_p[x, y]$ such that $f(x, y) = g(x, y) \cdot h(x, y)$. One can assume without loss of generality that $\deg_x(g(x, y)) \geqslant \deg_x(h(x, y))$, hence, $\deg_x(g(x, y)) = 2$ and $\deg_x(h(x, y)) = 1$. One can write $g(x, y) = g_2(y)x^2 + g_1(y)x + g_0$ and $h(x, y) = h_1(y)x + h_0(y)$ with $g_i(y), h_j(y) \in \overline{\mathbb{F}}_p[y]$ for $0 \leqslant i \leqslant 2$ and $0 \leqslant j \leqslant 1$. By comparing the degree of the polynomial in y in front of x^i in $f(x, y)$ with that in $g(x, y) \cdot h(x, y)$, one obtains $\deg_y(g_2(y)) = \deg_y(h_1(y)) = 0$, $\deg_y(g_1(y)) = \deg_y(h_0(y)) = 1$ and $\deg_y(g_0(y)) = 2$. Therefore, one can write the polynomials $g_i(y)$ and $h_i(y)$ as

$$g_0(y) = g_{02}y^2 + g_{01}y + g_{00}, \qquad g_1(y) = g_{11}y + g_{10}, \qquad g_2(y) = g_{20},$$

$$h_0(y) = h_{01}y + h_{00}, \qquad h_1(y) = h_{10}$$

with $g_{ij}, h_{ij} \in \overline{\mathbb{F}}_p$, where $g_{02}g_{11}g_{20}h_{01}h_{10} \neq 0$. By dividing $h(x, y)$ by h_{10} and multiplying $g(x, y)$ with it, one can assume that $h_{10} = 1$. A comparison of the polynomials in y in front of x^3 shows $g_{20} = c_1$. Likewise, the polynomial in front of x^0 leads to the equations

$$g_{02}h_{01} = c_2, \tag{6.9}$$

$$g_{00}h_{00} = a', \tag{6.10}$$

$$g_{02}h_{00} + g_{01}h_{01} = 0. \tag{6.11}$$

From (6.10), it follows that $g_{00}h_{00} \neq 0$, and hence, one obtains

$$h_{01} = \frac{c_2}{g_{02}}, \qquad h_{00} = \frac{a'}{g_{00}} \qquad \text{and} \qquad g_{01} = -\frac{a' g_{02}^2}{c_2 g_{00}}.$$

Comparing the polynomial in front of x^2 provides the equations

$$g_{20}h_{01} + g_{11}h_{10} = 0 \qquad \text{and} \qquad g_{20}h_{00} + g_{10}h_{10} = 0,$$

which can be combined with the previous equations to obtain

$$g_{11} = -\frac{c_1 c_2}{g_{02}} \qquad \text{and} \qquad g_{10} = -\frac{a' c_1}{g_{00}}.$$

The polynomial in front of x^1 leads to

$$g_{11}h_{01} + g_{02}h_{10} = 0 \qquad \text{and} \qquad g_{11}h_{00} + g_{10}h_{01} + g_{01}h_{10} = 0,$$

and combines with the previous equations to

$$g_{02}^3 = c_2^2 c_1 \qquad \text{and} \qquad g_{02}^3 = -2c_2^2 c_1,$$

which would lead to $3 = 0$. This is a contradiction to $p \equiv 1 \bmod 3$, which only holds for primes $p > 3$, hence the polynomial is absolute irreducible. □

LEMMA 29. *Let* $p \equiv 1 \bmod 3$, $a_1 - a_2 = p^\theta a'$, $a_1 \equiv a_2 \equiv 1 \bmod p$, $c_1, c_2, d_1, d_2 \in \mathbb{Z}$ *such that* $p \nmid c_1 c_2 d_1$, $d_1 \equiv 1 \bmod p$, *d_2 is congruent either to zero or one modulo p and* $c_1 \not\equiv b^3 c_2 \bmod p$ *for some* $b \in \mathbb{F}_p^*$. *Then the system of equations*

$$a_1 x_1^3 + a_2 x_2^3 + p^\theta \left(c_1 y_1^3 + c_2 y_2^3\right) = 0,$$

$$x_1 + x_2 + p^\theta \left(d_1 y_1 + d_2 y_2\right) = 0$$

has a non-trivial p-adic solution.

Proof. In the case that $d_2 \equiv 0 \bmod p$, set $x_1 = x + dp^\theta$ and $x_2 = -x$. This transforms the system of equation into

$$a' x^3 p^\theta + 3a_1 x^2 d p^\theta + 3a_1 x d^2 p^{2\theta} + a_1 d^3 p^{3\theta} + p^\theta \left(c_1 y_1^3 + c_2 y_2^3\right) = 0,$$

$$dp^\theta + p^\theta \left(d_1 y_1 + d_2 y_2\right) = 0.$$

Dividing both by p^θ, they have, modulo p, the form

$$a' x^3 + 3dx^2 + c_1 y_1^3 + c_2^3 y_2^3 \equiv 0 \bmod p,$$

$$d + y_1 \equiv 0 \bmod p.$$

Now setting $d \equiv -y_1 \bmod p$ and $y_2 = 1$ solves the lower equation modulo p and transforms the upper equation into

$$x^3 a' - 3y_1 x^2 + c_1 y_1^3 + c_2 \equiv 0 \bmod p.$$

It follows from Lemma 27 that this always has a solution. This solution is non-singular, as it holds $c_1 y_1^2 d_2 - c_2 y_2^2 d_1 \equiv -c_2 d_1 \not\equiv 0 \bmod p$.

In the case $d_2 \equiv 1 \bmod p$, setting $x_1 = 1 + dp^\theta$ and $x_2 = -1$ and dividing both the cubic and the linear equation by p^θ transform the system, modulo p, into

$$\begin{aligned} a' + 3d + c_1 y_1^3 + c_2 y_2^3 &\equiv 0 \bmod p, \\ d + y_1 + y_2 &\equiv 0 \bmod p. \end{aligned} \tag{6.12}$$

Setting $d \equiv -y_1 - y_2$ solves the lower equation modulo p and transforms the upper one into

$$a' - 3y_1 - 3y_2 + c_1 y_1^3 + c_2 y_2^3 \equiv 0 \bmod p. \tag{6.13}$$

If N is the number of solution of this equation, it follows, because the equation is absolute irreducible, due to Lemma 28, with Lemma 26 that

$$N \geqslant p - \left[2\sqrt{p}\right] - 2.$$

Every solution of this equation solves the system of equations above. If $c_1 y_1^2 - c_2 y_2^2 \not\equiv 0 \bmod p$, this solution can be lifted to a non-trivial p-adic solution. Else $c_1 y_1^2 \equiv c_2 y_2^2 \bmod p$ has to be fulfilled. The number of pairs (y_1, y_2) which fulfils this and solves the system is at most six because the equivalence is fulfilled if

$$y_1^2 \equiv \frac{c_2}{c_1} y_2^2,$$

which has no solution; if $\left(\frac{c_1 c_2}{p}\right) = -1$, and if $\left(\frac{c_1 c_2}{p}\right) = 1$, it follows that there is a b such that $y_1 \equiv \pm b y_2 \bmod p$. Putting this in (6.13), one obtains

$$a' \mp 3by_2 - 3y_2 \pm c_1 b^3 y_2^3 + c_2 y_2^3 \equiv 0 \bmod p,$$

which has at most three solution in both cases. Hence, if $N > 6$, there is at least one non-trivial p-adic solution. Solving $p - \left[2\sqrt{p}\right] - 2 > 6$, one obtains that there are at least seven solutions if $p \geqslant 17$. The remaining primes for which a non-singular solution of (6.13) has to be found are 7 and 13. It follows from the assumption of this lemma that $[c_1] \neq [c_2]$. Every solution of this equation with $0 \not\equiv y_1 \equiv \pm y_2 \bmod p$ is a non-singular solution of the system of equation, because in that case $c_1 y_1^2 - c_2 y_2^2 \equiv (c_1 - c_2) y_1^2 \not\equiv 0 \bmod p$. Setting $y_2 = -y_1 \not\equiv 0 \bmod p$, one obtains a solution if $[c_1 - c_2] = [a']$. Furthermore, if (6.13) has a solution, which is non-singular as a solution of the system (6.12), for fixed values of c_1, c_2, and a', the same holds if the values of c_1 and c_2 are swapped or if a' is replaced by $-a'$. Hence, it suffices to show that there is a non-singular solution for all triples (c_1, c_2, a') with $c_1, c_2 \in \{1, \dots, p-1\}$ with $c_1 < c_2$, $[c_1] \neq [c_2]$, $[c_1 - c_2] \neq [a']$ and $a' \in \left\{1, \dots, \frac{p-1}{2}\right\}$.

p = 7: By setting either $y_1 = 0$ or $y_2 = 0$, one obtains that if one, c_1 or c_2, is equivalent to $x \pm a'$ for $x \in \{3, 5, 6\}$, there is a non-singular solution. Furthermore, by setting $y_1 \equiv y_2 \not\equiv 0 \bmod p$, one obtains a non-singular solution also if $c_1 + c_2 \equiv x \pm a'$ for x as before. For all values of (c_1, c_2, a') not excluded above, one of this possibilities provides a non-singular solution.

p = 13: Again, by setting either y_1 or $y_2 = 0$, one obtains that if one, c_1 or c_2, is equivalent to $x \pm a'$ for $x \in \{1, 3, 9\}$ or $x \pm 5a'$ for $x \in \{4, 10, 12\}$, there is a non-singular solution. Setting $y_1 = y_2 \not\equiv 0 \bmod p$ provides a non-singular solution if $c_1 + c_2 \equiv x \pm a'$ for $x \in \{2, 5, 6\}$ and if $c_1 + c_2 \equiv x \pm 8a'$ for $x \in \{7, 8, 11\}$. Here, for each value of a', there is one pair (c_1, c_2), which gets not excluded in this way. The following table provides these problematic triples, together with values for y_1 and y_2 which provide a non-singular solution.

a'	c_1	c_2	y_1	y_2	a'	c_1	c_2	y_1	y_2
1	3	6	5	1	4	1	2	7	1
2	4	8	1	5	5	7	10	7	1
3	5	9	9	1	6	11	12	1	2

Hence, all the remaining primes do have a non-singular solution as well, which can be lifted with Lemma 5 to a non-trivial p-adic solution. □

LEMMA 30. *A critical system with $\theta = 3v + r$ where $0 \leqslant r \leqslant 2$, for which $\mu_i > \theta - v$ for $2r + 3 \leqslant i \leqslant 2r + 4$ holds has a non-trivial p-adic solution.*

Proof. Set all variables 0 except x_1, x_2, x_{2r+3} and x_{2r+4}. This transforms the system into

$$a_1x_1^3 + a_2x_2^3 + p^r \quad \left(c_1x_{2r+3}^3 + c_2x_{2r+4}^3\right) = 0,$$
$$x_1 + \quad x_2 + p^{\theta-v+1}\left(d_1x_{2r+3} + d_2x_{2r+4}\right) = 0,$$

where $p^rc_i = a_{2r+2+i}$ and $p^{\theta-v+1}d_i = b_{2r+2+i}$ for $1 \leqslant i \leqslant 2$, hence, $p \nmid c_i$. Setting $x_{2r+2+i} = p^vz_i$ for $1 \leqslant i \leqslant 2$, one obtains

$$a_1x_1^3 + a_2x_2^3 + p^\theta \quad \left(c_1z_1^3 + c_2z_2^3\right) = 0,$$
$$x_1 + \quad x_2 + p^{\theta+1}\left(d_1z_1 + d_2z_2\right) = 0.$$

Due to Conclusion 1 and Lemma 8, one can choose $(x, z_1, z_2) \not\equiv (0, 0, 0) \bmod p$ such that $a'x^3 + c_1z_1^3 + c_2z_2^3 \equiv 0 \bmod p$. As at least one of x, z_1 and z_2 is not equivalent to 0, and they fulfil the equation, it follows that at least two of them are not equivalent to 0. After swapping z_1 and z_2 if necessary, one can assume that $z_1 \not\equiv 0 \mod p$. Set $x_1 = x$ and $x_2 = -x + (-d_1z_1 - d_2z_2)p^{\theta+1}$. The equation

$$\varphi(t) := p^{-\theta}\left(a_1x^3 + a_2\left(-x + (-d_1t - d_2z_2)p^{\theta+1}\right)^3\right) + c_1t^3 + c_2z_2^3$$

has, modulo p, a zero at z_1, whereas $\varphi'(z_1) \equiv 3c_1z_1^2 \not\equiv 0 \bmod p$. Hensel's Lemma provides $\tilde{z}_1$ with $\varphi(\tilde{z}_1) = 0$ in $\mathbb{Q}_p$. This is equivalent to

$$a_1x^3 + a_2\left(-x + (-d_1z_1 - d_2z_2)p^{\theta+1}\right)^3 + p^\theta\left(c_1\tilde{z}_1^3 + c_2z_2^3\right) = 0,$$
$$x + \left(-x + (-d_1z_1 - d_2z_2)p^{\theta+1}\right) + p^{\theta+1}\left(d_1\tilde{z}_1 + d_2z_2\right) = 0,$$

which proves the claim. □

LEMMA 31. *A critical system with $\theta < 3$ has a non-trivial p-adic solution.*

Proof. By the definition of a critical system, it follows that $\theta \geqslant 1$, hence, $x_{2\theta+3}$ and $x_{2\theta+4}$ are all variables with $\nu_i = \theta$. Suppose that for all $i \in \{2\theta + 3, 2\theta + 4\}$ it holds $\mu_i > \theta$. Then Lemma 30 yields the desired non-trivial p-adic solution. If there is an $i \in \{2\theta + 3, 2\theta + 4\}$ with $\mu_i < \theta$, then x_i is a low variable at level less than θ. Therefore, Lemma 24 gives a non-trivial p-adic solution. It remains the cases with $\mu_i \geqslant \theta$ for $i \in \{2\theta + 3, 2\theta + 4\}$ and $\mu_i = \theta$ for at least one of them. This case is solved with Lemma 29. □

For the remainder of this chapter, some new notation is needed. Denote for $\tau \in \mathbb{N}_0$ with $\tau = 3u + \rho$, where $0 \leqslant \rho \leqslant 2$ and $u \in \mathbb{N}_0$

$$A(\mathbf{x}) = \sum_{i=1}^{8} a_ix_i^3, \qquad A_\tau(\mathbf{x}) = A(x_1, x_2, p^{u+1}y_0, \ldots, p^{u+1}y_\rho, p^uy_{\rho+1}, \ldots, p^uy_2),$$

$$B(\mathbf{x}) = \sum_{i=1}^{8} b_ix_i, \qquad B_\tau(\mathbf{x}) = B(x_1, x_2, p^{u+1}y_0, \ldots, p^{u+1}y_\rho, p^uy_{\rho+1}, \ldots, p^uy_2),$$

where $y_i = (x_{2i+3}, x_{2i+4})$. The system $A_\tau(\mathbf{x}) = B_\tau(\mathbf{x}) = 0$ is equivalent to $A(\mathbf{x}) = B(\mathbf{x}) = 0$, hence, it suffices to find a non-trivial p-adic solution for $A_\tau(\mathbf{x}) = B_\tau(\mathbf{x}) = 0$ for some τ.

Denote by $a_i^{(\tau)}$ and $b_i^{(\tau)}$ the coefficients of the system $A_\tau(\mathbf{x}) = B_\tau(\mathbf{x}) = 0$, and let $p^{\nu_i^{(\tau)}} \| a_i^{(\tau)}$ and $p^{\mu_i^{(\tau)}} \| b_i^{(\tau)}$.

LEMMA 32. *A critical system with $\mu_i > \nu_i$ for all $i \geqslant 3$ has a non-trivial p-adic solution.*

Proof. Let $\theta = 3v + r$ with $0 \leqslant r \leqslant 2$. It follows from the definition of $\nu_i^{(\tau)}$ and $\mu_i^{(\tau)}$ that for τ big enough $\nu_i^{(\tau)} > \mu_i^{(\tau)}$ for all $i \geqslant 3$. Let t be the smallest integer possible such that there exists an $i \geqslant 3$ such that $\nu_i^{(t)} \geqslant \mu_i^{(t)}$. In the case that $t > \theta - 3$, it follows from the definition of t that $\nu_i^{(\theta-3)} < \mu_i^{(\theta-3)}$ for all $i \geqslant 3$. Furthermore, for all $i \in \{2r+3, 2r+4\}$, one has $\nu_i^{(\theta-3)} = \nu_i + 3(v - 1 + 1) = r + 2v = \theta$, $\mu_i^{(\theta-3)} = \mu_i + v - 1 + 1 = \mu_i + v$ and therefore, $\mu_i > \theta - v$. Hence, Lemma 30 provides a non-trivial p-adic solution. It remains the case with $t \leqslant \theta - 3$. Write $t = 3u' + \rho'$ with $0 \leqslant \rho' \leqslant 2$. As t was chosen smallest possible, it follows that $i \in \{2\rho' + 3, 2\rho' + 4\}$ for those i with $\mu_i^{(t)} \leqslant \nu_i^{(t)}$. Define

$$\beta := \min\left\{\mu_i^{(t)} : \mu_i^{(t)} \leqslant \nu_i^{(t)}\right\} = \min\left\{\mu_i^{(t)} : 2\rho' + 3 \leqslant i \leqslant 2\rho' + 4\right\}.$$

For the $i \in \{2\rho' + 3, 2\rho' + 4\}$, it holds $\nu_i^{(t)} = \rho' + 3(u' + 1) = t + 3$, hence, $\beta \leqslant t + 3 \leqslant \theta$. Writing $\beta = 3u'' + \rho''$ with $0 \leqslant \rho'' \leqslant 2$, one can choose an $i' \in \{2\rho' + 3, 2\rho' + 4\}$ with $\mu_{i'}^{(t)} = \beta$. Suppose $\mu_{i'}^{(t)} < \nu_{i'}^{(t)}$, and hence, $\beta < t + 3 \leqslant \theta$. By the minimality of t, it follows that $\nu_{i'}^{(t-1)} < \mu_{i'}^{(t-1)}$. However, $\nu_{i'}^{(t)} = \nu_{i'}^{(t-1)} + 3$ and $\mu_{i'}^{(t)} = \mu_{i'}^{(t-1)} + 1$, such that $\nu_{i'}^{(t)} - 3 < \mu_{i'}^{(t)} - 1$ and hence, $t < \beta - 1 < t + 2$ and therefore, $\beta = t + 2$ and $\rho'' \equiv \rho' + 2 \bmod 3$. In both cases, if $\rho'' = \rho' + 2$ and $u'' = u'$ and if $\rho'' = \rho' - 1$ and $u'' = u' + 1$, it follows for $i \in \{2\rho'' + 3, 2\rho'' + 4\}$ that $\nu_i^{(t)} = \beta$ and, due to the definition of t, $\mu_i^{(t)} > \nu_i^{(t)} = \beta$ can be deduced. Setting all variables in $A_t(\mathbf{x})$ and $B_t(\mathbf{x})$ to 0, except x_1, x_2, $x_{i'}$ and $y_{\rho''}$, provides a system as in Lemma 23, and hence, a non-trivial p-adic solution exists.

The remaining case, $\mu_{i'}^{(t)} = \nu_{i'}^{(t)}$, and hence, $\beta = t + 3$, can be divided into different cases again. If $\beta = t + 3 = \theta$ or $\beta = t + 3 < \theta - 2$, one sets all variables in $A_t(\mathbf{x})$ and $B_t(\mathbf{x})$ to 0 except x_1, x_2 and $y_{\rho'}$. For all $i \in \{2\rho' + 3, 2\rho' + 4\}$, it holds $\nu_i^{(t)} \leqslant \mu_i^{(t)}$ with at least one equality and hence, the system turns into

$$a_1 x_1^3 + a_2 x_2^3 + p^{t+3}\left(c_1 x_{2\rho'+3}^3 + c_2 x_{2\rho'+4}^3\right) = 0,$$

$$x_1 + \quad x_2 + p^{t+3}\left(d_1 x_{2\rho'+3} + d_2 x_{2\rho'+4}\right) = 0.$$

This system has a non-trivial p-adic solution, which follows either by Lemma 29 or Lemma 25. Now, let $\beta = t + 3 = \theta - k$ for $k \in \{1, 2\}$. Set everything 0 except x_1, x_2, $y_{\rho'}$ and y_r. As before, $\mu_i^{(t)} \geqslant \nu_i^{(t)}$ for all $i \in \{2\rho' + 3, 2\rho' + 4\}$. It is easy to verify that $\nu_i^{(t)} = \theta - k$ for $i \in \{2\rho' + 3, 2\rho' + 4\}$ and $\nu_j^{(t)} = \theta - 3$ for all $j \in \{2r + 3, 2r + 4\}$ by differencing between the different values of k and ρ'. Let, without loss of generality, be $\mu_{2r+3} \leqslant \mu_{2r+4}$, hence, $\mu_{2r+3}^{(\tau)} \leqslant \mu_{2r+4}^{(\tau)}$ for all $\tau \in \mathbb{N}_0$. It follows from Lemma 30 that, if no non-trivial p-adic solution exists, $\theta - v \geqslant \mu_{2r+3}$. Assuming $k = 1$, it follows that $\mu_{2r+3}^{(t)} = \mu_{2r+3} + u'$ for $r \in \{1, 2\}$, where $u' = v - 1$, and $\mu_{2r+3}^{(t)} = \mu_{2r+3} + u' + 1$ for $r = 0$, where $u' = v - 2$. If $\mu_{2r+3} < \theta - v$, by transforming $y_r \mapsto p^{\theta - v - \mu_{2r+3}} y_r$, one obtains

$$\tilde{\nu}_{2r+3}^{(t)} = \nu_{2r+3}^{(t)} + 3\left(\theta - v - \mu_{2r+3}\right) \geqslant \nu_{2r+3}^{(t)} + 3 = \theta,$$

$$\tilde{\mu}_{2r+3}^{(t)} = \mu_{2r+3}^{(t)} + \theta - v - \mu_{2r+3} = \theta - 1.$$

Therefore, in setting $x_{2r+4} = 0$, the system $A_t(x) = B_t(x) = 0$ becomes

$$a_1x_1^3 + a_2x_2^3 + p^{\theta-1}\left(c_1x_{2\rho'+3}^3 + c_2x_{2\rho'+4}^3\right) + p^{\theta+2}dx_{2r+3} = 0,$$

$$x_1 + \quad x_2 + p^{\theta-1}\left(d_1x_{2\rho'+3} + d_2x_{2\rho'+4}\right) + p^{\theta-1}ex_{2r+3} = 0,$$

which can be solved with Lemma 23. For $\mu_{2r+3} = \theta - v$, applying $y_r \mapsto py_r$ gives $\tilde{\mu}_{2r+3}^{(t)} = \mu_{2r+3}^{(t)} + 1 = \theta$ and $\tilde{\nu}_{2r+4}^{(t)} = \tilde{\nu}_{2r+3}^{(t)} = \nu_{2r+3}^{(t)} + 3 = \theta$. Setting $y_{\rho'} = 0$, one obtains

$$a_1x_1^3 + a_2x_2^3 + p^{\theta}\left(c_1x_{2r+3}^3 + c_2x_{2r+4}^3\right) = 0,$$

$$x_1 + x_2 + p^{\theta}\left(d_1x_{2r+3} + d_2x_{2r+4}\right) = 0,$$

which can be solved with Lemma 29. It remains the case $k = 2$. Here, for $r \in \{0, 1\}$, it follows that $\mu_{2r+3}^{(t)} = \mu_{2r+3} + u' + 1$, where $u' = v - 2$ and for $r = 2$ that $\mu_{2r+3}^{(t)} = \mu_{2r+3} + u'$, where $u' = v - 1$, which can be combined to obtain $\mu_{2r+3}^{(t)} = \mu_{2r+3} + v - 1$. Due to the minimality of t, because of $\theta - 3 = \nu_{2r+3}^{(t)}$ and $\mu_{2r+3} \geqslant \theta - v$, it follows that

$$\theta - 3 < \mu_{2r+3}^{(t)} = \mu_{2r+3} + v - 1 \leqslant \theta - 1,$$

hence, it suffices to regard the cases $\mu_{2r+3}^{(t)} = \theta - 1$ and $\mu_{2r+3}^{(t)} = \theta - 2$. For $\mu_{2r+3}^{(t)} = \theta - 1$, setting $y_{\rho'} = 0$ and applying $y_r \mapsto py_r$ transform the system into

$$a_1x_1^3 + a_2x_2^3 + p^{\theta}\left(c_1x_{2r+3}^3 + c_2x_{2r+4}^3\right) = 0,$$

$$x_1 + x_2 + p^{\theta}\left(d_1x_{2r+3} + d_2x_{2r+4}\right) = 0,$$

which, again, can be solved via Lemma 29. For $\mu_{2r+3}^{(t)} = \theta - 2$, applying $y_r \mapsto py_r$ and $y_{\rho'} \mapsto py_{\rho'}$ provides a system with $\tilde{\nu}_{2r+i}^{(t)} = \theta$, $\tilde{\mu}_{2r+3}^{(t)} = \theta - 1$, $\tilde{\nu}_{2\rho'+i}^{(t)} = \theta + 1$ and $\tilde{\mu}_{2\rho'+i}^{(t)} \geqslant \theta - 1$ for $i \in \{3, 4\}$, where $\tilde{\mu}_{2\rho'+l}^{(t)} = \theta - 1$ holds for $2\rho' + l = i'$ with some $l \in \{3, 4\}$. Setting $x_1 = 1 = -x_2$, one obtains a system of the form

$$a'p^{\theta} + p^{\theta+1}\left(c_1x_{2\rho'+3}^3 + c_2x_{2\rho'+4}^3\right) + p^{\theta} \quad \left(e_1x_{2r+3}^3 + e_2x_{2r+4}^3\right) = 0,$$

$$p^{\theta-1}\left(d_1x_{2\rho'+3} + d_2x_{2\rho'+4}\right) + p^{\theta-1}\left(f_1x_{2r+3} + f_2x_{2r+4}\right) = 0.$$

Multiplying the cubic equation with $p^{-\theta}$ and the linear one with $p^{-\theta+1}$, one obtains, modulo p, the system

$$a' + e_1x_{2r+3}^3 + e_2x_{2r+4}^3 \equiv 0 \bmod p,$$

$$d_1x_{2\rho'+3} + d_2x_{2\rho'+4} + f_1x_{2r+3} + f_2x_{2r+4} \equiv 0 \bmod p.$$

It is always possible to solve the cubic equation modulo p with $x_{2r+i} \not\equiv 0 \bmod p$ for at least one $i \in \{3, 4\}$, say j, due to Conclusion 1 and Lemma 8. The linear equation can be solved by setting the remaining variable, which is not $x_{2\rho'+l}$ to 0 and choosing $x_{2\rho'+l}$ accordingly. This solution is non-singular, because $e_{j-2}x_{2r+j}^2d_{l-2} - c_{l-2}x_{2\rho'+l}^2f_{j-2} \equiv e_{j-2}x_{2r+j}d_{l-2} \not\equiv 0 \bmod p$. Hence, it can be lifted to a non-trivial p-adic solution with Lemma 5. □

LEMMA 33. *A critical system with $\theta \geqslant 5$ has a non-trivial p-adic solution.*

Proof. If $\mu_i > \nu_i$ for all $i \geqslant 3$, a non-trivial p-adic solution is provided by Lemma 32. If $\mu_i < \nu_i$ for some $i \geqslant 3$, this is a low variable at a level smaller than θ and hence, Lemma 24 provides a non-trivial p-adic solution. In the remaining cases, it holds $\mu_i \geqslant \nu_i$ for all $i \geqslant 3$

and $\mu_j = \nu_j$ for at least one $j \geqslant 3$, but it follows from the definition of a critical system that $\mu_3 > \nu_3 = 1$ and $\mu_4 > \nu_4$ and hence, $\mu_j = \nu_j$ for at least some $j \geqslant 5$. For this j, it holds $1 \leqslant \mu_j = \nu_j \leqslant 2 = 5 - 3 \leqslant \theta - 3$, hence, Lemma 25 provides a solution. □

It remains the two cases $\theta = 3$ and $\theta = 4$ which will be handled in the next two lemmata.

LEMMA 34. *A critical system with $\theta = 4$ has a non-trivial p-adic solution.*

Proof. If $\mu_i > \nu_i$ for all $i \geqslant 3$, the system can be solved with Lemma 32 and if there is an $i \geqslant 3$ with $\mu_i < \nu_i$, a non-trivial p-adic solution is provided by Lemma 24. As before, one already knows $\mu_i > \nu_i$ for $3 \leqslant i \leqslant 4$. If $\mu_i = \nu_i$ for some $5 \leqslant i \leqslant 6$, a solution exists due to Lemma 25. To sum it up, the remaining cases have got $\mu_i > \nu_i$ for $3 \leqslant i \leqslant 6$ and at least one of $i \in \{7, 8\}$ with $\mu_i = \nu_i$. Without loss of generality, one can assume that $\mu_7 = \nu_7 = 2$, $\mu_8 \geqslant \nu_8 = 2$ and $\mu_5 \leqslant \mu_6$. If $\mu_5 > \theta - v = 4 - 1 = 3$, then Lemma 30 provides a non-trivial p-adic solution, hence, one can assume $2 \leqslant \mu_5 \leqslant 3$. In the case $\mu_5 = 3$, applying $y_1 \mapsto py_1$ transforms the system into one with $\mu_5 = 3 + 1 = \theta$ and $\nu_5 = \nu_6 = 1 + 3 = \theta$ and hence, Lemma 29 provides a non-trivial p-adic solution. The remaining case with $\mu_5 = 2$ can be changed by applying $y_1 \mapsto py_1$ and $y_2 \mapsto py_2$ into one with $\mu_5 = 3$, $\nu_5 = \nu_6 = 4$, $\mu_7 = 3$ and $\nu_7 = \nu_8 = 5$. Setting $x_1 = 1$, $x_2 = -1$, $x_3 = x_4 = x_8 = 0$ and multiplying the cubic equation with p^{-4} and the linear one with p^{-3}, one obtains

$$a' + \tilde{a}_5 x_5^3 + \tilde{a}_6 x_6^3 \equiv 0 \bmod p,$$

$$\tilde{b}_5 x_5 + \tilde{b}_6 x_6 + \tilde{b}_7 x_7 \equiv 0 \bmod p.$$

Solving the cubic equation modulo p such that $x_i \not\equiv 0 \bmod p$ for some $i \in \{5, 6\}$ and using x_7 to solve the linear equation modulo p give a solution which can be lifted to a non-trivial p-adic solution with Lemma 5 because $\tilde{a}_i x_i^2 \tilde{b}_7 - p\tilde{a}_7 x_7^2 \tilde{b}_i \equiv \tilde{a}_i x_i^2 \tilde{b}_7 \not\equiv 0 \bmod p$. This solves the case $\theta = 4$. □

LEMMA 35. *A critical system with $\theta = 3$ has a non-trivial p-adic solution.*

Proof. If $\mu_i > \nu_i$ for all $i \geqslant 3$, Lemma 32 provides a non-trivial p-adic solution. Likewise, Lemma 24 provides one if $\mu_i < \nu_i$ for some $i \geqslant 3$. Without loss of generality, one can assume that $\mu_3 \leqslant \mu_4$, $\mu_5 \leqslant \mu_6$ and $\mu_7 \leqslant \mu_8$. If $\mu_3 > \theta - v = 2$, a non-trivial p-adic solution exists due to Lemma 30, hence one can assume that $1 \leqslant \mu_3 \leqslant 2$. Assume $\mu_5 > \nu_5 = 1$. Then $\mu_6 > \nu_6 = 1$ as well and it follows $\mu_7 = \nu_7 = 2$ because for at least one $i \geqslant 3$ it has to hold that $\mu_i = \nu_i$. If furthermore, $\mu_3 = 2$, by applying $y_0 \mapsto py_0$ one obtains a system with $\mu_3 = \nu_3 = \nu_4 = \theta$, which can be solved with Lemma 29. Hence, $\mu_3 = 1$. Such a system can be transformed with $y_0 \mapsto py_0$ into one with $\mu_3 = 2$ and $\nu_3 = 3$. As $\mu_7 = \nu_7 = \nu_8 = 2$, this is solvable with Lemma 23.

It remains the case with $1 = \mu_5 = \nu_5$. Here, for $\mu_3 = 2$, applying $y_0 \mapsto py_0$ transforms the system into one with $\mu_3 = \nu_3 = \theta$, and hence, the system can be solved with Lemma 29. For $\mu_3 = 1$, applying $y_0 \mapsto py_0$ and $y_1 \mapsto py_1$ transforms it into a system with $\mu_3 = \nu_3 = \theta$ $\mu_5 = 2$ and $\nu_5 = 4$. Setting $x_1 = 1$, $x_2 = -1$, $x_6 = x_7 = x_8 = 0$ and multiplying the cubic equation with p^{-3} and the linear one with p^{-2}, the systems has, modulo p, the form

$$a' + \tilde{a}_3 x_3^3 + \tilde{a}_4 x_4^3 \equiv 0 \bmod p,$$

$$\tilde{b}_3 x_3 + \tilde{b}_4 x_4 + \tilde{b}_5 x_5 \equiv 0 \bmod p.$$

One can solve the cubic equation modulo p such that $x_i \not\equiv 0 \bmod p$ for some $i \in \{3, 4\}$ and use x_5 to solve the linear one modulo p. This solution modulo p can be lifted with Lemma 5 to a non-trivial p-adic solution because $\tilde{a}_i x_i^2 \tilde{b}_5 - \tilde{a}_5 x_5^2 \tilde{b}_i \equiv \tilde{a}_i x_i \tilde{b}_5 \not\equiv 0 \bmod p$. □

Hence, every system with $(v_0, t) = (4, 2)$ has a non-trivial p-adic solution.

§7. *The cases* $(v_0, t) = (4, 3)$ *and* $(v_0, t) = (4, 4)$. One has to find a non-singular solution of the system

$$a_1x_1^3 + a_2x_2^3 + a_3x_3^3 + a_4x_4^3 \equiv 0 \bmod p,$$

$$b_1x_1 + b_2x_2 + b_3x_3 + b_4x_4 \equiv 0 \bmod p,$$

with $a_1a_2a_3a_4b_1b_2b_3 \not\equiv 0 \bmod p$, where, dependent on the value of (v_0, t), either $p \mid b_4$ or $p \nmid b_4$. If such a solution exists, it can be lifted to a non-trivial p-adic solution with Lemma 5. Applying $x_i \mapsto b_i^{-1}x_i$ for those b_i with $1 \leqslant i \leqslant 4$ where $p \nmid b_i$, one can assume that b_i is equivalent to 1 or 0 for $1 \leqslant i \leqslant 4$. Starting with the case $(v_0, t) = (4, 3)$, one has to solve the system

$$\begin{aligned} a_1x_1^3 + a_2x_2^3 + a_3x_3^3 + a_4x_4^3 &\equiv 0 \bmod p, \\ x_1 + x_2 + x_3 &\equiv 0 \bmod p. \end{aligned} \tag{7.1}$$

Due to Lemma 14, one can assume that a_1, a_2 and a_3 are distinct modulo p, else a non-singular solution exists. If the system can be solved with $x_4 \not\equiv 0 \bmod p$, then $a_4x_4^2b_1 - a_1x_1^2b_4 \equiv a_4x_4^2 \not\equiv 0 \bmod p$, and hence, the solution is non-singular. Setting $x_2 = 1$ and $x_3 = -1 - x_1$ solves the linear equation modulo p and transforms the cubic one into

$$(a_1 - a_3)x_1^3 - 3a_3x_1^2 - 3a_3x_1 + a_2 - a_3 + a_4x_4^3 \equiv 0 \bmod p. \tag{7.2}$$

There can be at most three solution of (7.2) with $x_4 = 0$ because this is a polynomial of degree 3 over a field. Hence, if there are at least four solutions of (7.2), at least one of them has to be non-singular. To estimate the number of solution, one can use Lemma 26 again. For that, one needs to show that (7.2) is absolute irreducible. The following lemma will be very useful in doing just that.

LEMMA 36. *Suppose the polynomial* $y^d - f(x)$ *has coefficients in a field* k. *Then the following three conditions are equivalent.*

(i) $y^d - f(x)$ *is absolutely irreducible.*
(ii) $y^d - cf(x)$ *is absolutely irreducible for every* $c \neq 0$, $c \in k$.
(iii) *If* $f(x) = a(x - \alpha_1)^{d_1} \cdots (x - \alpha_m)^{d_m}$ *is the factorisation of* f *in* $\overline{k}$, *with* $\alpha_i \neq \alpha_j$ *for* $i \neq j$, *then* $(d, d_1, \ldots, d_m) = 1$.

Proof. See [**10**, Lemma 2C]. □

LEMMA 37. *The function* $f(x, y) = (a_1 - a_3)x^3 - 3a_3x^2 - 3a_3x + a_2 - a_3 + a_4y^3$ *is absolute irreducible.*

Proof. Define $g(x)$ via

$$a_4^{-1}f(x, y) = y^3 - \big(a_4^{-1}(a_3 - a_1)x^3 + 3a_4^{-1}a_3x^2 + 3a_4^{-1}a_3x + a_4^{-1}(a_3 - a_2)\big) =: y^3 - g(x).$$

Let $g(x) = \frac{a_3 - a_1}{a_4}(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ be the factorisation of g in $\overline{\mathbb{F}}_p$. Either all α_i with $1 \leqslant i \leqslant 3$ are equal, or at least one of the zeros is simple. If all three are equal, a comparison of the coefficients shows $\alpha_i = -a_3(a_3 - a_1)^{-1}$ and $\alpha_i^2 = a_3(a_3 - a_1)^{-1}$ which can be combined to conclude $a_1 = 0$, which is a contradiction, hence, at least one of the zeros is simple. Therefore, the third equivalence of Lemma 36 is fulfilled and hence, $a_4^{-1} f(x, y)$ is irreducible as well as $f(x, y)$. □

Applying Lemma 26 to the function $f(x, y)$, one obtains $N \geqslant p - \left[2\sqrt{p}\right] - 2$, and therefore, $N > 3$ for all $p > 11$. It remains to show that a solution of the system (7.1) with $x_4 \not\equiv 0 \bmod 7$ exists. Showing that it is possible to choose x_1, x_2 and x_3 such that $[a_1x_1^3 + a_2x_2^3 + a_3x_3^3] = [a_4]$ while $x_1 + x_2 + x_3 \equiv 0 \bmod 7$ is equivalent to show that the system (7.1) has a solution, because it enables one to choose $x_4 \not\equiv 0 \bmod 7$ such that the system is solved. Multiplying the cubic equation with a_4^{-1}, one can assume that $a_4 \equiv 1 \bmod 7$. Denoting by $\tilde{a}_i$ the representant of a_i modulo 7 with $1 \leqslant \tilde{a}_i \leqslant 6$, there have to be $i, j \in \{1, 2, 3\}$ with $i \neq j$ such that $\tilde{a}_i$ and $\tilde{a}_j$ are either both in $\{1, 2, 3\}$ or both in $\{4, 5, 6\}$. One can apply $x_l \mapsto -x_l$ for $1 \leqslant i \leqslant 3$ and multiply the linear equation by -1 to obtain a system as before, where the sign of a_1, a_2 and a_3 has changed. This changes the set in which $\tilde{a}_i$ and $\tilde{a}_j$ are in. By applying this transformation, if necessary, one can assume that they are both in $\{1, 2, 3\}$. By permutating the first three variables, if necessary, one obtains a system with $1 \leqslant \tilde{a}_1 < \tilde{a}_2 \leqslant 3$ and $\tilde{a}_2 < \tilde{a}_3 \leqslant 6$.

If $\tilde{a}_2 - \tilde{a}_1 = 1$, setting $x_1 = -1$, $x_2 = 1$ and $x_3 = 0$ provides the desired solution, hence, one can assume that $\tilde{a}_1 = 1$, $\tilde{a}_2 = 3$ and $\tilde{a}_3 \in \{4, 5, 6\}$. For each of these cases, one can choose $(x_1, x_2, x_3) \in \{(0, -1, 1), (1, 1, 5), (3, 2, 2)\}$ such that $[a_1x_1^3 + a_2x_2^3 + a_3x_3^3] = [a_4]$ while $x_1 + x_2 + x_3 \equiv 0 \bmod 7$, which proves the case $p = 7$.

For $(v_0, t) = (4, 4)$, one has to solve the system of equations

$$\begin{aligned} a_1x_1^3 + a_2x_2^3 + a_3x_3^3 + a_4x_4^3 &\equiv 0 \bmod p, \\ x_1 + x_2 + x_3 + x_4 &\equiv 0 \bmod p. \end{aligned} \tag{7.3}$$

If $a_i \equiv a_j \bmod p$ for some $1 \leqslant i < j \leqslant 4$, the system can be solved due to Lemma 14. Hence, from now on, one can assume that a_1, a_2, a_3 and a_4 are distinct modulo p. Setting $x_4 = -x_1 - x_2 - x_3$ solves the linear system. For $A_i := a_i - a_4$ for $i \in \{1, 2, 3\}$ and $a := a_4$, by setting either $x_1 = 1$ or $x_3 = 1$, the cubic equation transforms in either

$$A_2x_2^3 - 3a(1 + x_3)x_2^2 - 3a\left(1 + 2x_3 + x_3^2\right)x_2 + A_3x_3^3 - 3ax_3^2 - 3ax_3 + A_1 \equiv 0 \bmod p \tag{7.4}$$

or

$$A_2x_2^3 - 3a(1 + x_1)x_2^2 - 3a\left(1 + 2x_1 + x_1^2\right)x_2 + A_1x_1^3 - 3ax_1^2 - 3ax_1 + A_3 \equiv 0 \bmod p. \tag{7.5}$$

The conditions on the a_i transform into $A_i \neq A_j$ for $i \neq j$, $a \neq 0$, $a + A_i \neq 0$ and $A_i \neq 0$ for $1 \leqslant i \leqslant 3$ and the following lemma shows that at least one of them is absolute irreducible over $\mathbb{F}_p$.

LEMMA 38. *If $A_i \neq A_j$, for $i \neq j$, $a \neq 0$, $a + A_i \neq 0$ and $A_i \neq 0$ for $1 \leqslant i, j \leqslant 3$, at least one of the polynomials*

$$f_1(x, y) = A_2x^3 - 3a(1 + y)x^2 - 3a\big(1 + 2y + y^2\big)x + A_3y^3 - 3ay^2 - 3ay + A_1$$

and

$$f_2(x, y) = A_2x^3 - 3a(1 + y)x^2 - 3a\big(1 + 2y + y^2\big)x + A_1y^3 - 3ay^2 - 3ay + A_3,$$

is absolute irreducible in $\mathbb{F}_p$

Proof. Let $f(x,y) = Ax^3 - 3a(1+y)x^2 - 3a\big(1+2y+y^2\big)x + By^3 - 3ay^2 - 3ay + C$. If $f(x,y)$ is not absolute irreducible, there are $g(x,y), h(x,y) \in \overline{\mathbb{F}}_p[x,y]$ such that $f(x,y) = g(x,y) \cdot h(x,y)$. Then $\deg_x(g(x,y)) + \deg_x(h(x,y)) = 3$. Without loss of generality, one can assume that $\deg_x(g(x,y)) \geqslant \deg_x(h(x,y))$, hence, $\deg_x(g(x,y)) = 2$ and $\deg_x(h(x,y)) = 1$. One can write $g(x,y) = g_2(y)x^2 + g_1(y)x + g_0(y)$ and $h(x,y) = h_1(y)x + h_0(y)$ with $g_i(y), h_j(y) \in \overline{\mathbb{F}}_p[y]$ for $0 \leqslant i \leqslant 2$ and $0 \leqslant j \leqslant 1$, which provides the equations

$$\begin{aligned} g_2(y)h_0(y) + g_1(y)h_1(y) &= -3a(1+y), & g_2(y)h_1(y) &= A, \\ g_1(y)h_0(y) + g_0(y)h_1(y) &= -3a\big(1+2y+y^2\big), & g_0(y)h_0(y) &= By^3 - 3ay^2 - 3ay + C, \end{aligned} \tag{7.6}$$

where one can compare the degree in y to obtain

$$\deg(g_0(y)) = 2, \quad \deg(g_1(y)) \in \{0,1\}, \quad \deg(g_2(y)) = 0, \quad \deg(h_0(y)) = 1,$$
$$\deg(h_1(y)) = 0,$$

and hence,

$$\begin{aligned} g_0(y) &= g_{02}y^2 + g_{01}y + g_{00}, & g_1(y) &\in \{g_{10}, g_{11}y + g_{10}\}, & g_2(y) &= g_{20}, \\ h_0(y) &= h_{01}y + h_{00}, & h_1(y) &= h_{10}, \end{aligned}$$

with $g_{02}g_{10}g_{20}h_{01}h_{10} \neq 0$ or $g_{02}g_{11}g_{20}h_{01}h_{10} \neq 0$, depending on the degree of $g_1(y)$. By multiplying $g(x,y)$ with g_{20}^{-1} and $h(x,y)$ with g_{20}, one can, without loss of generality, assume that $g_{20} = 1$. If $\deg(g_1(y)) = 0$, expanding the left-hand side of (7.6) and comparing the coefficients in front of the powers of y, one obtains

$$h_{10} = A, \qquad h_{01} = -3a, \qquad h_{00} = -3a - Ag_{10}, \qquad g_{02} = -\frac{3a}{A},$$

which can be combined with the fourth equation of (7.6), to obtain $9a^2 = AB$. If both functions, $f_1(x,y)$ and $f_2(x,y)$, can be written as a product of functions $g_i(x,y)h_i(x,y) = f_i(x,y)$, the corresponding functions $g_1^{(i)}(y)$ have to have degree 0 or 1. If they are 0 in both cases, it follows that $A_2A_1 = 9a^2 = A_2A_3$ and hence, $A_1 = A_3$, which contradicts the assumption. It follows that at most one of the functions $f_i(x,y)$ can have a corresponding function $g_1^{(i)}(y)$ with degree 0. Hence, one can choose $f(x,y)$ as one of the equation $f_i(x,y)$ with $9a^2 \neq AB$. If this equation is not absolute irreducible, it follows that $\deg(g_1(y)) = 1$. Here, expanding the left-hand side of the first three of equations (7.6) and comparing the coefficients in front of the powers of y gives

$$\begin{aligned} h_{10} &= A, & h_{01} &= -3a - Ag_{11}, & h_{00} &= -3a - Ag_{10}, \\ g_{00} &= -\frac{3a}{A} + \frac{3a}{A}g_{10} + g_{10}^2, & g_{01} &= -\frac{6a}{A} + \frac{3a}{A}g_{10} + \frac{3a}{A}g_{11} + 2g_{10}g_{11}, & g_{02} &= -\frac{3a}{A} + \frac{3a}{A}g_{11} + g_{11}^2. \end{aligned}$$

By combing them with the fourth one, one obtains

$$9a^2 - 9a^2g_{11} + 3aAg_{11} - 6aAg_{11}^2 - A^2g_{11}^3 = AB, \tag{7.7}$$

$$9a^2 - 9a^2g_{10} + 3aAg_{10} - 6aAg_{10}^2 - A^2g_{10}^3 = AC, \tag{7.8}$$

$$g_{10}\big(-aA + 3a^2 + 4aAg_{11} + A^2g_{11}^2\big) = 9a^2 + aA + 2aAg_{11} - 6a^2g_{11} - 2aAg_{11}^2, \tag{7.9}$$

$$g_{11}\big(-aA + 3a^2 + 4aAg_{10} + A^2g_{10}^2\big) = 9a^2 + aA + 2aAg_{10} - 6a^2g_{10} - 2aAg_{10}^2. \tag{7.10}$$

Assuming $g_{10} = 0$, the equation (7.10) transforms to $g_{11}(-A + 3a) = 9a + A$. As $g_{11} \neq 0$, either $3a - A = 9a + A = 0$ or both are not 0. If both are 0, it follows that $3a = A = -9a$

and hence $a = 0$, which contradicts the assumption. Hence, $3a - A \neq 0$ and $9a + A \neq 0$. Plugging $g_{11} = \frac{9a+A}{3a-A}$ and $g_{10} = 0$ into (7.9), one obtains

$$-3a(a+A)(3a+A)(9a+A) = 0.$$

As 3, a, $9a + A$ and $a + A$ are not 0, it follows that $-3a = A$. Plugging in $g_{10} = 0$ in (7.8) provides $9a^2 = AC$, hence, $9a^2 = -3aC$ and therefore $C = -3a = A$, which contradicts the assumption. From that one can conclude that $g_{10} \neq 0$. Assume that the equation

$$9a + A + 2Ag - 6ag - 2Ag^2 = 0 \tag{7.11}$$

for $g \in \{g_{10}, g_{11}\}$ holds. As both g_{10} and g_{11} are not 0, one can conclude from (7.9) and (7.10) that

$$-aA + 3a^2 + 4aAg + A^2g^2 = 0. \tag{7.12}$$

Combining both equations, one obtains $g = \frac{-6a-A}{2A}$, which plugged into (7.12) provides $A = 0$ contradicting the assumption. Hence, $9a + A + 2Ag - 6ag - 2Ag^2 \neq 0$ for $g \in \{g_{10}, g_{11}\}$. Therefore, solving (7.9) and (7.10) for g_{10} and g_{11}, respectively, one obtains

$$g_{10} = \frac{9a^2 + aA + 2aAg_{11} - 6a^2g_{11} - 2aAg_{11}^2}{-aA + 3a^2 + 4aAg_{11} + A^2g_{11}^2},$$

$$g_{11} = \frac{9a^2 + aA + 2aAg_{10} - 6a^2g_{10} - 2aAg_{10}^2}{-aA + 3a^2 + 4aAg_{10} + A^2g_{10}^2},$$

hence, it is possible to write each g_{10} and g_{11} as a function of the other one. Inserting one function into the other, one obtains for $g \in \{g_{10}, g_{11}\}$ the equation

$$\begin{aligned}&-a(a+A)\big(-81a^4 - 36a^3A - 3a^2A^2 + 81a^4g - 54a^3Ag - 24a^2A^2g - aA^3g\\ &\quad + 108a^3Ag^2 - 4aA^3g^2 + 54a^2A^2g^3 + 6aA^3g^3 + 12aA^3g^4 + A^4g^4 + A^4g^5\big) = 0,\end{aligned}$$

which is, as $a \neq 0$ and $a + A \neq 0$, equivalent to

$$\begin{aligned}&-81a^4 - 36a^3A - 3a^2A^2 + 81a^4g - 54a^3Ag - 24a^2A^2g - aA^3g\\ &\quad + 108a^3Ag^2 - 4aA^3g^2 + 54a^2A^2g^3 + 6aA^3g^3 + 12aA^3g^4 + A^4g^4 + A^4g^5 = 0.\end{aligned} \tag{7.13}$$

By bringing g^3 to one side of (7.7) and (7.8) and putting this into (7.13), one obtains for $(g, D) \in \{(g_{10}, C), (g_{11}, B)\}$

$$-A(a+D)\big(9a^2 + A^2g + A^2g^2 + 3aA + 6aAg^2\big) = 0,$$

and because $A \neq 0$ and $a + D \neq 0$ that

$$g^2 = -\frac{9a^2 + 3aA + A^2g + 6aAg}{A^2},$$

which, inserting into (7.7) and (7.8), provides

$$g = -\frac{3a + D}{A}.$$

If one puts this into the (7.7) and (7.8), one obtains, again for $(g, D) \in \{(g_{10}, C), (g_{11}, B)\}$, the equation

$$(-A + D)D(3a + A + D) = 0,$$

but as $A \neq D$ and $D \neq 0$, it follows that

$$C = -3a - A = B,$$

which contradicts the assumption. Hence, neither $f_1(x, y)$ nor $f_2(x, y)$ can be the product of $g(x, y)h(x, y)$ with $\deg(g_1(y)) = 1$ and at most one of them can have $\deg(g_1(y)) = 0$, hence, at least one of them is absolute irreducible. □

It follows from the previous Lemma that one can set either $x_1 = 1$ or $x_3 = 1$ such that the cubic equation transforms into an absolute irreducible polynomial. Due to Lemma 26, the number of solution N of this polynomial can be estimated through $N \geqslant p - \left[2\sqrt{p}\right] - 2$. Let $i, j \in \{1, 3\}$, $i \neq j$, such that $x_i = 1$ provides an absolute irreducible polynomial. Then $a_i x_i^2 b_2 - a_2 x_2^2 b_i \equiv a_i - a_2 x_2^2$. If this is not equivalent to 0 modulo p for a solution of the absolute irreducible polynomial, then the solution is a non-singular solution of the system, which can be lifted to a non-trivial p-adic solution. For $a_i - a_2 x_2^2 \equiv 0 \bmod p$, there exists at most two values of x_2 which can solve this equation, and for each of them there can be at most three values of x_j, which solves the absolute irreducible polynomial. Hence, if there are at least seven solutions of the absolute irreducible polynomial, at least one does not solve the equation $a_i - a_2 x_2^2 \equiv 0 \bmod p$ and hence, there is at least one non-singular solution, which can be lifted to a non-trivial p-adic solution, as needed. Therefore, if $p - \left[2\sqrt{p}\right] - 2 > 6$, which holds for $p \geqslant 17$, the case is solved. It remains the cases $p = 7$ and $p = 13$, which will be handled using the following lemmata.

LEMMA 39. *Let $1 \leqslant i, j, k, l \leqslant 4$ be all distinct with $[a_i - a_j] = [a_k - a_l]$. Then the system (7.3) has a non-trivial p-adic solution.*

Proof. Setting $x_i = 1$, $x_j = -1$, $x_k = x$ and $x_l = -x$ solves the linear equation and transforms the cubic one into

$$(a_i - a_j) + (a_k - a_l)x^3 \equiv 0 \bmod p,$$

which can be solved non-trivially due to $[a_i - a_j] = [a_k - a_l]$. Furthermore, $a_i x_i^2 b_j - a_j x_j^2 b_i \equiv a_i - a_j \not\equiv 0 \bmod p$ because a_1, a_2, a_3 and a_4 are distinct modulo p, hence, the solution is non-singular and can be lifted due to Lemma 5. □

LEMMA 40. *Let $1 \leqslant i, j, k, l \leqslant 4$ all distinct with $[a_i] = [a_j]$ and $[a_k] = [a_l]$. Then the system (7.3) has a non-trivial p-adic solution.*

Proof. As the a_i for $1 \leqslant i \leqslant 4$ are all distinct and all non-zero modulo p, it follows that there are b and c not equivalent to 0 or 1 modulo p such that $a_i \equiv b^3 a_j \bmod p$ and $a_k \equiv c^3 a_l \bmod p$. Setting $x_j = b, x_i = -1, x_l = cx$ and $x_k = -x$ solves the cubic equation and reduces the linear one to

$$(b - 1) + (c - 1)x \equiv 0 \bmod p,$$

which can be solved by choosing x appropriate as $c - 1$ is not zero. This solution is non-singular, because $a_j x_j^2 - a_i x_i^2 \equiv a_j b^2 (1 - b)$ which is not equivalent to 0 modulo p because a_j, b and $1 - b$ are not equivalent to 0 modulo p. Hence, due to Lemma 5, the system has a non-trivial p-adic solution. □

There are only three classes for $[a_i]$, hence, it follows that at least two of them are in the same class. Furthermore, due to Lemma 40, one can assume that the other two are not in the same class, therefore, after renumbering if necessary, either $[a_1] = [a_2] = [a_3] \neq [a_4]$ or $[a_1] = [a_2]$ while a_3 and a_4 are in the two remaining classes. Multiplying the cubic equation with a_1^{-1} does not change this relation. For $p = 7$, only the second case can occur, because there are only two elements in every equivalence class. Hence, one can assume that $a_1 \equiv 1 \bmod 7$ and $a_2 \equiv 6 \bmod 7$ while a_3 is congruent to 2 or 5 modulo 7 and a_4 to 3 or 4. If $[a_2 - a_1] = [a_3 - a_4]$, there is also a solution due to Lemma 39, hence it remains the cases $(a_3, a_4) \in \{(2, 3), (5, 4)\}$ which can be solved non-trivial with $(x_1, x_2, x_3, x_4) \in \{(5, 1, 1, 0), (1, 5, 1, 0)\}$.

For $p = 13$, if $[a_1] = [a_2] = [a_3]$, it follows that a_2 and a_3 are congruent to 5, 8, or 12 and a_4 is congruent to one element of the set $\{2, 3, 4, 6, 7, 9, 10, 11\}$. As before, one can assume without loss of generality that $a_2 \leqslant a_3$. Those cases which cannot be solved with Lemma 39 are solved in the following table.

a_2	a_3	a_4	x_1	x_2	x_3	x_4	a_2	a_3	a_4	x_1	x_2	x_3	x_4	a_2	a_3	a_4	x_1	x_2	x_3	x_4
5	8	6	10	1	0	2	5	12	4	1	1	0	11	8	12	2	5	1	0	7
5	8	7	3	1	0	9	5	12	9	5	0	1	7	8	12	4	3	1	0	9
5	8	10	8	1	0	4	5	12	11	0	1	5	7	8	12	9	4	1	0	8

If $[a_1] = [a_2]$ but a_3 and a_4 are in the two remaining equivalence classes with $[a_3] \neq [a_4]$, one can assume that a_3 is equivalent to an element in the set $\{2, 3, 10, 11\}$ and a_4 to one in $\{4, 6, 7, 9\}$. Most of these cases can be solved with Lemma 39 and the remaining ones with their solution modulo 13 can be seen in the following table.

a_2	a_3	a_4	x_1	x_2	x_3	a_4	a_2	a_3	a_4	x_1	x_2	x_3	a_4	a_2	a_3	a_4	x_1	x_2	x_3	a_4
5	2	7	7	1	5	0	8	3	4	2	1	10	0	12	3	4	4	1	8	0
5	3	6	11	1	1	0	8	10	7	4	0	3	6	12	10	9	10	1	2	0
5	10	7	8	1	4	0	8	10	9	0	3	8	2	12	11	4	6	1	0	6
5	11	6	10	1	0	2	8	11	9	6	1	6	0	12	11	7	2	1	0	10
5	11	9	12	0	2	12	12	2	6	11	0	1	1							
8	2	4	5	1	7	0	12	2	9	5	1	0	7							

Hence, for $p = 7$ and $p = 13$, all cases have a non-trivial solution modulo p. Those solution are even non-singular, because every solution has at least one of the $x_i = 0$ for some $1 \leqslant i \leqslant 4$, and one $x_j \not\equiv 0 \bmod p$ for $1 \leqslant j \leqslant 4$. Hence, $a_j x_j^2 b_i - a_i x_i^2 b_j \equiv a_j x_j^2 \not\equiv 0 \bmod p$ shows that these solutions can be lifted to a non-trivial p-adic one. This completes the case $(v_0, t) = (4, 4)$ and with that the case $p \equiv 1 \bmod 3$. Finally, some more attention has to be paid to the case $p = 3$.

§8. *The case* $p = 3$. As three divides every partial differential of the cubic equation, to prove the existence of a non-trivial p-adic solution, one has to solve the cubic equation modulo 9, while for the linear one three suffices, as stated in Lemma 5. To show that a non-singular solution for a system (4.1) exists, the parameters used in the previous section are not precise enough. Hence, the following notation is required.

For $0 \leqslant i \leqslant 2$, define

$$X_{i0} := \left\{x_k \mid k \in \{1, \ldots, s\}, 3^i \parallel a_k, 3 \nmid b_k\right\}, \qquad X_{i1} := \left\{x_k \mid k \in \{1, \ldots, s\}, 3^i \parallel a_k, 3 \mid b_k\right\},$$

and the partial unions $X_i := X_{i0} \cup X_{i1}$. The cardinality of these sets $t_{ij} := \#X_{ij}$ and the partial sums $v_i := t_{i0} + t_{i1} = \#X_i$ are adequate to describe a system (4.1) for this proof.

In the proof of Lemma 11, the basics of this idea were already used. By mapping a system (4.1) to an equivalent one with a non-trivial 3-adic solution, one proves that it has one as well.

The following three transformations are a finite series of the processes introduced in § 4. They map subsets of the set of systems (4.1) to the set of systems (4.1).

(i) Apply $x_i \mapsto 3x_i$ for all $x_i \in X_0$ and multiply the cubic equation by $\frac{1}{3}$.

(ii) If $t_{20} = 0$, multiply the cubic equation by 3 and apply $x_i \mapsto \frac{1}{3}x_i$ for all $x_i \in X_2$.

(iii) If $t_{10} + t_{20} = 0$, multiply the cubic equation by 9 and apply $x_i \mapsto \frac{1}{3}x_i$ for all $x_i \in X_1 \cup X_2$.

The second and the third transformation cannot be applied to every system (4.1), as if the condition is not fulfilled, then the systems turns into one with non-integer coefficients. A system (4.1) which gets mapped by one of these transformations to a system with a non-trivial 3-adic solution has one as well, because they are equivalent to each other. By applying one of the transformations, one can therefore extend the set of systems (4.1) having a confirmed non-trivial 3-adic solution.

The following lemmata will proof that systems (4.1) with specific parameters have a non-trivial 3-adic solution, which will be combined to show that all ordered conditioned systems (4.1) are covered by these systems.

Lemma 41. *If $c_1, c_2, c_3 \in (\mathbb{Z}/9\mathbb{Z})^*$ are pairwise distinct, it is possible to choose two of them such that the difference is congruent to 3 modulo 9 and, by swapping the minuend and the subtrahend, to 6 modulo 9.*

Proof. In $(\mathbb{Z}/9\mathbb{Z})^*$, only two residue classes modulo 3 are contained. Therefore, at least two c_i have to be in the same residue class. Those two are not equal, hence, they differ by 3 or 6. □

Lemma 42. *A system (4.1) with $t_{00} + t_{10} + t_{20} \geqslant 3$ and $1 \leqslant i < j \leqslant t_{00}$ such that $a_i \equiv a_j \bmod 9$ has a non-trivial 3-adic solution.*

Proof. Set $x_i = 1$, $x_j = -1$ and the remaining variables 0. Hence, the system (4.1) turns into

$$a_i x_i^3 + a_j x_j^3 \equiv a_i - a_j \equiv 0 \bmod 9,$$

$$x_i + x_j \equiv 1 - 1 \equiv 0 \bmod 3.$$

There is a variable $x_k \in X_{00} \cup X_{10} \cup X_{20} \backslash \{x_i, x_j\}$ which has the value 0. It follows that $b_k a_i x_i^2 - b_i a_k x_k^2 \equiv a_i \not\equiv 0 \bmod 3$ and hence, Lemma 5 provides the wanted solution. □

Lemma 43. *A system (4.1) with $t_{00} + t_{10} + t_{20} \geqslant 1$ and $a_i \equiv a_j \bmod 9$ for some $t_{00} + 1 \leqslant i < j \leqslant v_0$ has a non-trivial 3-adic solution.*

Proof. Set $x_i = 1$, $x_j = -1$ and the remaining variables 0. This solves the cubic equation modulo 9 and the linear one modulo 3. There is a variable $x_k \in X_{00} \cup X_{10} \cup X_{20}$ with $x_k = 0$. It follows that $b_k a_i x_i^2 - b_i a_k x_k^2 \equiv a_i \not\equiv 0 \bmod 3$ and hence, Lemma 5 can be applied to obtain a non-trivial 3-adic solution. □

Lemma 44. *A system (4.1) with $t_{00} \geqslant 5$ has a non-trivial 3-adic solution.*

Proof. One can assume that the a_i corresponding to those $x_i \in X_{00}$ are all distinct modulo 9, because else, Lemma 42 provides a non-trivial 3-adic solution.

Since $t_{00} \geqslant 5$, it follows from Lemma 41 that it is possible to choose $x_i, x_j \in X_{00}$ such that $a_i - a_j \equiv 3 \bmod 9$. The remaining elements in X_{00} are still at least 3. Lemma 41 can be applied again to provide $x_k, x_l \in X_{00}\backslash\{x_i, x_j\}$ such that $a_k - a_l \equiv 6 \bmod 9$. Taking $x_i = x_k = 1$, $x_j = x_l = -1$ and setting the remaining variables 0 provides a solution for both the cubic and linear equation. Since there is at least one variable, say x_m, in X_{00} which was set 0, one gets $b_m a_i x_i^2 - b_i a_m x_m^2 \equiv a_i \not\equiv 0 \bmod 3$ and therefore a non-trivial 3-adic solution can be obtained by Lemma 5. □

By applying transformation (i) to a system (4.1) with $t_{10} \geqslant 5$, it becomes an equivalent system (4.1) with $t_{00} \geqslant 5$.

Conclusion 2. A system (4.1) with $t_{10} \geqslant 5$ has a non-trivial 3-adic solution.

LEMMA 45. *An ordered system* (4.1) *with* $v_0 \geqslant 4$ *and* $t_{20} \geqslant 1$ *has a non-trivial* 3*-adic solution.*

Proof. Choose $x_i \in X_{20}$ and set every variable 0 except $x_1, \ldots, x_4$ and x_i. One can choose $x_1, \ldots, x_4$ in a way that the cubic equation is congruent to 0 modulo 9. If either two of the corresponding coefficients are equivalent modulo 9, then one can set one of them 1, the other one -1 and the remaining 0. Otherwise, at least one of the sets $\{1, 8\}$, $\{2, 7\}$ and $\{4, 5\}$ is completely represented by $x_1, \ldots, x_4$ modulo 9. Choose these two, set both 1 and the remaining 0. In either case, there is a variable, say x_j, among $x_1, \ldots, x_4$ which is 1. Now set x_i such that the linear equation is congruent to 0 modulo 3. This does not change the value of the cubic equation modulo 9. Since $b_i a_j x_j^2 - b_j a_i x_i^2 \equiv a_j \not\equiv 0 \bmod 3$, it follows from Lemma 5 that there is a non-trivial 3-adic solution. □

Setting $x_i = 0$ for all $x_i \in X_{10} \cup X_{20}$ turns a system (4.1) with $t_{11} \geqslant 4$ and $t_{00} \geqslant 1$ into one with $t_{10} + t_{20} = 0$. Then transformation (iii) can be applied to change it into an system (4.1) with $v_0 \geqslant 4$ and $t_{20} \geqslant 1$. After renumbering to obtain an ordered system, Lemma 45 provides a non-trivial p-adic solution.

Conclusion 3. A system (4.1) with $t_{11} \geqslant 4$ and $t_{00} \geqslant 1$ has a non-trivial 3-adic solution.

LEMMA 46. *An ordered system* (4.1) *with* $v_0 \geqslant 2$, $v_1 \geqslant 1$ *and* $t_{20} \geqslant 1$ *has a non-trivial* 3*-adic solution.*

Proof. Let $x_i \in X_1$ and $x_j \in X_{20}$. Set all variables 0 except x_1, x_2, x_i and x_j. Now set $x_1 = 1$ and choose $x_2 \in \{-1, 1\}$ such that $a_1 x_1^3 + a_2 x_2^3 \equiv 0 \bmod 3$. This is always possible since both a_1 and a_2 are congruent to either 1 or 2 modulo 3. Now one can choose $x_i \in \{0, 1, -1\}$ in a way that the cubic equation is congruent to 0 modulo 9 because $a_i \in \{3, 6\}$ modulo 9. To make the linear equation congruent to 0 modulo 3, one can choose x_j suitably, without changing the value of the cubic equation modulo 9. Furthermore, $b_j a_1 x_1^2 - b_1 a_j x_j^2 \equiv a_1 \not\equiv 0 \bmod 3$ ensures that one can lift the solution with Lemma 5 to a non-trivial 3-adic one. □

To apply transformation (ii) or (iii) to a system (4.1) with $v_0 \geqslant 1$, $t_{10} \geqslant 1$ and $t_{21} \geqslant 2$ or $t_{11} \geqslant 2, t_{21} \geqslant 1$ and $t_{00} \geqslant 1$, one has to set $x_i = 0$ for all $x_i \in X_{20}$ or $x_i \in X_{10} \cup X_{20}$, respectively. It then becomes an equivalent system (4.1) with $v_0 \geqslant 2$, $v_1 \geqslant 1$ and $t_{20} \geqslant 1$, which can be renumbered to obtain an ordered system (4.1) with the same parameters.

Conclusion 4. A system (4.1) with $v_0 \geqslant 1$, $t_{10} \geqslant 1$ and $t_{21} \geqslant 2$ has a non-trivial 3-adic solution.

Conclusion 5. A system (4.1) with $t_{11} \geqslant 2$, $t_{21} \geqslant 1$ and $t_{00} \geqslant 1$ has a non-trivial 3-adic solution.

LEMMA 47. *A system* (4.1) *with* $t_{00} \geqslant 3$ *and* $t_{11} \geqslant 1$ *has a non-trivial* 3*-adic solution.*

Proof. If there are $x_i, x_j \in X_{00}$ such that $a_i \equiv a_j \bmod 9$, it follows from Lemma 42 that a non-trivial 3-adic solution exists, else all the corresponding coefficients of $x_i \in X_{00}$ are distinct. There is an $x_k \in X_{11}$, hence, from the definition of X_{11} it follows that a_k is congruent to 3 or 6 modulo 9. With that in mind one can choose, due to Lemma 41, $a_i, a_j \in X_{00}$ such that $a_i - a_j \equiv -a_k \bmod 9$. Now setting $x_i = x_k = 1$ and $x_j = -1$ and the remaining variables 0 solves the cubic equation modulo 9 and the linear one modulo 3. There is an $x_l \in X_{00}$ which was set 0. The lift of the solution follows by Lemma 5 because $b_l a_i x_i^2 - b_i a_l x_l^2 \equiv a_i \not\equiv 0 \bmod 3$. □

By applying transformation (i) to a system (4.1) with $t_{10} \geqslant 3$ and $t_{21} \geqslant 1$, it becomes an equivalent system (4.1) with $t_{00} \geqslant 3$ and $t_{11} \geqslant 1$.

Conclusion 6. A system (4.1) with $t_{10} \geqslant 3$ and $t_{21} \geqslant 1$ has a non-trivial 3-adic solution.

LEMMA 48. *A system* (4.1) *with* $t_{01} \geqslant 2$, $t_{11} \geqslant 1$ *and* $t_{00} + t_{10} + t_{20} \geqslant 1$ *has a non-trivial* 3*-adic solution.*

Proof. Let $x_i, x_j \in X_{01}$, $x_k \in X_{11}$ and set every variable except these three 0. Then the linear equation is solved modulo 3 independent of the value of these variables. It is possible to choose $x_i, x_j \in \{1, -1\}$ in a way that $a_i x_i^3 + a_j x_j^3 \equiv 0 \bmod 3$ and $x_k \in \{0, 1, -1\}$ that the cubic equation is solved modulo 9, because a_k is congruent to 3 or 6 modulo 9 per definition of X_{11}. There is also an $x_l \in X_{00} \cup X_{10} \cup X_{20}$ with $x_l = 0$. One sees that $b_l a_i x_i^2 - b_i a_l x_l^2 \equiv a_i \not\equiv 0 \bmod 3$ and hence, the solution is liftable to a non-trivial 3-adic one by Lemma 5. □

By applying transformation (i) to a system (4.1) with $t_{11} \geqslant 2$, $t_{21} \geqslant 1$ and $t_{10} + t_{20} \geqslant 1$, it becomes an equivalent system (4.1) with $t_{01} \geqslant 2$, $t_{11} \geqslant 1$ and $t_{00} + t_{10} + t_{20} \geqslant 1$.

Conclusion 7. A system (4.1) with $t_{11} \geqslant 2$, $t_{21} \geqslant 1$ and $t_{10} + t_{20} \geqslant 1$ has a non-trivial 3-adic solution.

LEMMA 49. *A system* (4.1) *with* $t_{00} \geqslant 3$ *and* $t_{01} \geqslant 2$ *has a non-trivial* 3*-adic solution.*

Proof. If there are $x_i, x_j \in X_{00}$ such that $a_i \equiv a_j \bmod 9$, Lemma 42 provides a non-trivial 3-adic solution. Let $x_i, x_j \in X_{01}$. If one of $a_i + a_j$ and $a_i - a_j$ is congruent to 0 modulo 9 set $x_i = 1$ and choose $x_j \in \{1, -1\}$ such that the cubic congruence is fulfilled. Else $a_i + a_j$ or $a_i - a_j$ is congruent to 3 or 6 modulo 9 because a_i and a_j are congruent to 1 or 2 modulo 3. Set $x_i = 1$ and choose $x_j \in \{1, -1\}$ such that $a_i x_i^3 + a_j x_j^3 \equiv 0 \bmod 3$. Then Lemma 41 provides $x_k, x_l \in X_{00}$ with $a_k - a_l \equiv -a_i x_i^3 - a_j x_j^3 \bmod 9$. Therefore, one can set $x_k = 1$ and $x_l = -1$. In both cases, setting all the remaining variables 0 fulfils the cubic congruence modulo 9 and the linear modulo 3. There is an x_m in X_{00} which was set 0. Since $b_m a_i x_i^2 - b_i a_m x_m^2 \equiv a_i \not\equiv 0 \bmod 3$, this solution can be lifted to a non-trivial 3-adic one by Lemma 5. □

Apply transformation (i) to a system (4.1) with $t_{10} \geqslant 3$ and $t_{11} \geqslant 2$. It then becomes an equivalent system (4.1) with $t_{00} \geqslant 3$ and $t_{01} \geqslant 2$.

Conclusion 8. A system (4.1) with $t_{10} \geqslant 3$ and $t_{11} \geqslant 2$ has a non-trivial 3-adic solution.

LEMMA 50. *An ordered system* (4.1) *with* $t_{00} \geqslant 4$ *and* $t_{10} \geqslant 1$ *has a non-trivial* 3-*adic solution.*

Proof. One can assume that all a_i with $1 \leqslant i \leqslant t_{00}$ are distinct modulo 9 because otherwise Lemma 42 can be applied to show that there is a non-trivial 3-adic solution.

Permute the first four variables such that $a_1 \equiv \ldots \equiv a_{i_0}$ mod 3 and $a_1 \not\equiv a_{i_0+1} \equiv \ldots \equiv a_4$ mod 3. Modulo 9, there are three residue classes which are in the same residue class modulo 3, hence, $i_0 \in \{1, 2, 3\}$. If $i_0 = 2$, set $x_1 = -x_2 = 1$ and $x_3 = -x_4 = 1$ or $x_3 = -x_4 = -1$ such that the cubic equation is fulfilled and every other variable 0. This solves the cubic equation modulo 9 and the linear one modulo 3. This solution can be lifted by Lemma 5, since $b_3a_1x_1^2 - b_1a_3x_3^2 \equiv a_1 - a_3 \not\equiv 0$ mod 3.

Therefore, one can assume $i_0 \in \{1, 3\}$. In this case, modulo 9, one of the sets $\{1, 4, 7\}$ and $\{2, 5, 8\}$ is completely represented by $a_1, \ldots, a_4$ and the remaining coefficient lies in the other set. Hence, one can choose $i, j \in \{1, \ldots, 4\}$ such that $a_i + a_j$ is congruent to 3 modulo 9. Likewise one can choose them such that $a_i + a_j$ is congruent to 6 modulo 9. Therefore, choosing them such that $a_i + a_j$ is congruent to $-a_l$, where $x_l \in X_{10}$, one can set $x_i = x_j = x_l = 1$ and the remaining variables zero to solve the cubic equation modulo 9 and the linear one modulo 3. This solution can be lifted by Lemma 5, because $a_ix_i^2b_l - a_lx_l^2b_i \equiv a_i \not\equiv 0$ mod 3. □

LEMMA 51. *An ordered system* (4.1) *with* $t_{00} \geqslant 1$, $t_{01} \geqslant 3$ *and* $t_{10} \geqslant 2$ *has a non-trivial* 3-*adic solution.*

Proof. It follows from Lemma 43 that if there are $x_n, x_m \in X_{01}$ with $n \neq m$ and $a_n \equiv a_m$ mod 9, the system has a non-trivial 3-adic solution. Let $x_i, x_j \in X_{10}$. If $a_i \not\equiv a_j$ mod 9, set $x_i = -x_j = 1$. Lemma 41 can be applied to show that it is possible to choose $m, n \in X_{01}$ such that $a_m - a_n \equiv a_j - a_i$ mod 9. Setting $x_m = -x_n = 1$ and the remaining variables zero provides a non-singular solution, because $b_1a_nx_n^2 - b_na_1x_1^2 \equiv a_n \not\equiv 0$ mod 3, which can be lifted by Lemma 5 to a non-trivial 3-adic one.

Else $a_i \equiv a_j$ mod 9. If there is an a_n for $t_{00} + 1 \leqslant n \leqslant v_0$ such that $a_1 + a_i + a_j \equiv \pm a_n$ set $x_1 = x_i = x_j = 1$, $x_n = \mp 1$ and the remaining variables 0. This solves the cubic equation modulo 9 and the linear modulo 3, and can be lifted by Lemma 5, because $b_ia_1x_1^2 - b_1a_ix_i^2 \equiv a_1 \not\equiv 0$ mod 3. Else, all a_n for $t_{00} + 1 \leqslant n \leqslant v_0$ are neither congruent to $a_1 + a_i + a_j$ nor to $-a_1 - a_i - a_j$ modulo 9. But they have to be in the set $\{1, 2, 4, 5, 7, 8\}$, and since $a_1 + a_i + a_j$ is modulo 9 in one of the sets $\{1, 8\}$, $\{2, 7\}$ and $\{4, 5\}$, the a_n with $t_{00} + 1 \leqslant n \leqslant v_0$ have to be in the two remaining sets. They are distinct modulo 9, hence one of the sets is entirely represented. Therefore, there are $t_{00} + 1 \leqslant n < m \leqslant v_0$ with $a_n + a_m \equiv 0$ mod 9. Set $x_n = x_m = 1$ and the remaining variables 0. This is a non-singular solution because $b_1a_nx_n^2 - b_na_1x_1^2 \equiv a_n \not\equiv 0$ mod 3 and can be lifted to a non-trivial 3-adic solution by Lemma 5, which proves the lemma. □

LEMMA 52. *A system* (4.1) *with* $t_{01} \geqslant 4$ *and* $t_{00} + t_{10} + t_{20} \geqslant 1$ *has a non-trivial* 3-*adic solution.*

Proof. If there are $x_i, x_j \in X_{01}$ with $a_i \equiv a_j$ mod 9, Lemma 43 provides a non-trivial 3-adic solution. Else, at least one of the sets $\{1, 8\}$, $\{2, 7\}$ and $\{4, 5\}$ is by the a_i with $x_i \in X_{01}$

modulo 9 completely represented. It is therefore possible to choose $x_i, x_j \in X_{01}$ such that $a_i + a_j \equiv 0 \bmod 9$. Setting $x_i = x_j = 1$ and the remaining variables 0 provides a non-singular solution, which can be lifted by Lemma 5, because for $x_l \in X_{00} \cup X_{10} \cup X_{20}$ it follows that $b_l a_i x_i^2 - b_i a_l x_l^2 \equiv a_i \not\equiv 0 \bmod 3$. □

By applying transformation (i) to a system (4.1) with $t_{11} \geqslant 4$ and $t_{10} + t_{20} \geqslant 1$, it becomes a system (4.1) with $t_{01} \geqslant 4$ and $t_{00} + t_{10} + t_{20} \geqslant 1$.

Conclusion 9. A system (4.1) with $t_{11} \geqslant 4$ and $t_{10} + t_{20} \geqslant 1$ has a non-trivial 3-adic solution.

LEMMA 53. *An ordered system* (4.1) *with* $t_{00} \geqslant 2$, $t_{10} \geqslant 1$ *and* $t_{11} \geqslant 1$ *has a non-trivial* 3-*adic solution.*

Proof. Setting $x_1 = 1$, one can choose $x_2 \in \{\pm 1\}$, depending on whether a_1 and a_2 are in the same or in different equivalence classes modulo 3, such that $a_1 x_1^3 + a_2 x_2^3 \equiv 0 \bmod 3$. To solve the linear equation modulo 3, one chooses $x_{v_0+1} \in \{0, \pm 1\}$ and choosing $x_{v_0+t_{00}+1} \in \{0, \pm 1\}$ one can solve the cubic equation modulo 9 without changing the value of the linear equation. Setting all remaining variables 0, one obtains a non-singular solution, because $a_1 x_1^2 b_{v_0+1} - a_{v_0+1} x_{v_0+1}^2 b_1 \equiv a_1 \not\equiv 0 \bmod 3$, which can be lifted to a non-trivial 3-adic solution with Lemma 5. □

LEMMA 54. *An ordered system* (4.1) *with* $t_{00} \geqslant 3$, $t_{01} \geqslant 1$ *and* $t_{10} \geqslant 2$ *has a non-trivial* 3-*adic solution.*

Proof. One can assume that alle a_i with $1 \leqslant i \leqslant t_{00}$ are distinct modulo 9, because otherwise Lemma 42 provides a non-trivial 3-adic solution.

Set all variables 0 except $x_1, x_2, x_3, x_{t_{00}+1}, x_{v_0+1}$ and x_{v_0+2}. In the case $a_{v_0+1} \not\equiv a_{v_0+2} \bmod 9$, the coefficients a_1, a_2 and a_3 are either in the same equivalence class modulo 3, or one of them is in another class than the other two. If they are in the same class, it follows that $a_1 + a_2 + a_3 \equiv 0 \bmod 3$ but not equivalent to 0 modulo 9. Hence, setting $x_1 = x_2 = x_3 = 1$ and $x_{v_0+1} = \pm 1$ and $x_{v_0+2} = \mp 1$, dependent on whether $a_1 + a_2 + a_3$ is equivalent to 3 or to 6, solves the cubic equation modulo 9 and the linear one modulo 3. This is a non-singular solution because $a_1 x_1^2 b_{v_0+1} - a_{v_0+1} x_{v_0+1}^2 b_1 \equiv a_1 \bmod 3$. Else, without loss of generality, a_1 and a_2 are in the same equivalence class modulo 3 and a_3 in the other one. Therefore, it holds that $a_1 + a_3 \equiv a_2 + a_3 \equiv 0 \bmod 3$, but as $a_1 \not\equiv a_2 \bmod 9$, one can choose $i, j \in \{1, 2\}$ such that $a_i + a_3 \not\equiv 0 \bmod 9$, and $a_i + a_3 + a_{v_0+j} \equiv 0 \bmod 9$. Setting $x_i = x_3 = x_{v_0+j} = 1$ and everything else zero solves the cubic equation modulo 9 and the linear one modulo 3. This is non-singular, because $a_1 x_1^2 b_{v_0+j} - a_{v_0+j} x_{v_0+j}^2 b_1 \equiv a_1 \not\equiv 0 \bmod 3$.

Assume that $a_{v_0+1} \equiv a_{v_0+2} \bmod 9$ and define

$$A_{\mathbf{x}} := A(x_1, x_2, x_3, x_{t_{00}+1}) = a_1 x_1^3 + a_2 x_2^3 + a_3 x_3^3 + a_{t_{00}+1} x_{t_{00}+1}^3 \in \mathbb{Z}/9\mathbb{Z},$$

$$B_{\mathbf{x}} := B(x_1, x_2, x_3, x_{t_{00}+1}) = x_1 + x_2 + x_3 \in \mathbb{Z}/3\mathbb{Z}.$$

If it is possible to choose two vectors $\mathbf{x} = (x_1, x_2, x_3, x_{t_{00}+1}) \in \{0, 1, -1\}^4$, such that $A_{\mathbf{x}} \in \{3, 6\}$ and $B_{\mathbf{x}} \in \{1, 2\}$ where one of $A_{\mathbf{x}}$ and $B_{\mathbf{x}}$ has the same value for both vectors and the other one has two different values, one can set either both $x_{v_0+1} = x_{v_0+2} = 1$ or just $x_{v_0+1} = 1$ and $x_{v_0+2} = 0$. One of the settings of x_{v_0+1} and x_{v_0+2} together with one of the settings of $\mathbf{x}$ solves the cubic equation modulo 9 and the linear one modulo 3. As $x_1 + x_2 + x_3$ is in all cases equivalent to one or two, there is an $i \in \{1, 2, 3\}$ with $x_i \not\equiv 0 \bmod 3$. These solutions are non-singular, because $a_i x_i^2 b_{v_0+1} - a_{v_0+1} x_{v_0+1}^2 b_i \equiv a_i \not\equiv 0 \bmod 3$ and hence can be lifted to a non-trivial 3-adic one.

If a_1, a_2 and a_3 are in the same equivalent class modulo 3 and $a_{t_{00}+1}$ in the other, $a_i + a_{t_{00}+1}$ is congruent to 0, 3 and 6 modulo 9, depending on $i \in \{1, 2, 3\}$, hence setting $x_i = x_{t_{00}+1} = 1$ for those i which belongs to 3 or 6 and the other variables 0 provides $\left(A_{\mathbf{x}}, B_{\mathbf{x}}\right) = (3, 1)$ or $\left(A_{\mathbf{x}}, B_{\mathbf{x}}\right) = (6, 1)$, respectively, as needed. If $a_{t_{00}+1}$ is in the same equivalence class as a_1, a_2 and a_3, one can obtain (3,1) and (6,1) as well, because $a_i - a_{t_{00}+1}$ is equivalent to 0, 3 and 6, depending on $i \in \{1, 2, 3\}$ and hence setting $x_i = 1 = -x_{t_{00}+1}$ as above and the other variables 0 gives the desired result. From now on, one can assume without loss of generality a_1 and a_2 are in the same equivalence class modulo 3 and a_3 in the other. If a_3 is not equivalent to $-a_1$ and $-a_2$ modulo 9, setting $x_1 = x_3 = 1$ or $x_2 = x_3 = 1$ and the other variables 0 provides (3,2) and (6,2). Hence, one can assume without loss of generality that $a_3 \equiv -a_1 \bmod 9$. By multiplying the cubic equation with a_1^{-1}, one obtains $a_1 \equiv 1 \bmod 9$, $a_3 \equiv 8 \bmod 9$ and a_2 equivalent to either 4 or 7 modulo 9, while $a_{t_{00}+1} \in (\mathbb{Z}/9\mathbb{Z})^*$. The following table will prove the existence of the required vectors for the remaining cases.

a_2	$a_{t_{00}+1}$	x_1	x_2	x_3	$x_{t_{00}+1}$	$A_{\mathbf{x}}$	$B_{\mathbf{x}}$	a_2	$a_{t_{00}+1}$	x_1	x_2	x_3	$x_{t_{00}+1}$	$A_{\mathbf{x}}$	$B_{\mathbf{x}}$
4	1	0	1	0	−1	3	1	7	1	0	1	1	0	6	2
		1	1	−1	0	6	1			0	1	0	−1	6	1
4	2	1	0	0	1	3	1	7	2	0	1	1	0	6	2
		0	1	0	1	6	1			0	0	1	−1	6	1
4	4	0	0	1	1	3	1	7	4	0	1	1	0	6	2
		−1	1	1	1	6	1			1	0	0	−1	6	1
4	5	1	0	0	1	6	1	7	5	0	1	1	0	6	2
		0	0	1	−1	3	1			1	0	0	1	6	1
4	7	1	0	0	−1	3	1	7	7	0	1	1	0	6	2
		0	0	1	1	6	1			0	0	1	1	6	1
4	8	0	1	1	0	3	2	7	8	0	1	1	0	6	2
		0	1	0	1	3	1			0	1	0	1	6	1

□

LEMMA 55. *An ordered system* (4.1) *with* $t_{00} \geqslant 2$, $t_{01} \geqslant 2$ *and* $t_{10} \geqslant 2$ *has a non-trivial* 3*-adic solution.*

Proof. Assume $a_{t_{00}+1} \equiv \pm a_{t_{00}+2} \mod 9$. Then one can set $x_{t_{00}+1} = 1$ and choose $x_{t_{00}+2} \in \{\pm 1\}$ such that $a_{t_{00}+1} x_{t_{00}+1}^3 + a_{t_{00}+2} x_{t_{00}+2}^3 \equiv 0 \bmod 9$. Setting the remaining variables 0, one obtains a solution of the cubic equation modulo 9 and the linear one modulo 3. The solution is also non-singular because $a_{t_{00}+1} x_{t_{00}+1}^2 b_1 - a_1 x_1^2 b_{t_{00}+1} \equiv a_{t_{00}+1} \not\equiv 0 \bmod 3$ and therefore it can be lifted to a non-trivial 3-adic solution.

Hence, one may assume that $a_{t_{00}+1} \not\equiv \pm a_{t_{00}+2} \bmod 9$. Depending on them being in the same or in different equivalent classes modulo 3, either the difference or the sum of both is congruent to 0 modulo 3, but not to 0 modulo 9. It follows that for $n \in \{3, 6\}$ fixed, it is possible to choose $x_{t_{00}+1}, x_{t_{00}+2} \in \{\pm 1\}$ such that $a_{t_{00}+1} x_{t_{00}+2}^3 + a_{t_{00}+2} x_{t_{00}+2}^3 \equiv n \bmod 9$. Setting $x_1 = 1$ and choosing $x_2 \in \{\pm 1\}$ such that $a_1 x_1^3 + a_2 x_2^3 \equiv 0 \bmod 3$, one can choose $x_{v_0+1}, x_{v_0+2} \in \{0, 1\}$ such that the linear equation is equivalent to 0 modulo 3. Doing this does not change that the cubic equation is equivalent to 0 modulo 3. If it is also congruent to 0 modulo 9, this solves the system, else one can choose $x_{t_{00}+1}$ and $x_{t_{00}+2}$ as described above, to solve the cubic equation modulo 9, without changing the value of the linear equation modulo 3. This solution is non-singular, because $a_1x_1^2b_{v_0+1} - a_{v_0+1}x_{v_0+1}^2b_1 \equiv a_1 \not\equiv 0 \bmod 3$ and can be lifted to a non-trivial 3-adic solution with Lemma 5. □

The preceding lemmata and conclusions can be applied to prove Theorem 1 for $p = 3$.

LEMMA 56. *Every ordered conditioned system with $s \geqslant 8$ has a non-trivial 3-adic solution.*

Proof. From the definition of a conditioned system follows that one with $s \geqslant 8$ must fulfil the following four equations:

$$v_0 \geqslant 3, \tag{8.1}$$

$$v_0 + v_1 \geqslant 6, \tag{8.2}$$

$$s = v_0 + v_1 + v_2 \geqslant 8, \tag{8.3}$$

$$t_{00} + t_{10} + t_{20} \geqslant 1. \tag{8.4}$$

Assume there is a conditioned system (4.1) with $s \geqslant 8$ without a non-trivial 3-adic solution.

If this system has $t_{20} \geqslant 1$, Lemma 45 can be applied to show that $v_0 \leqslant 3$. From (8.1) and (8.2), it follows that $v_0 = 3$ and $v_1 \geqslant 3$, which contradicts with Lemma 46. Hence, t_{20} has to be 0.

Lemma 44 can be applied to show that $0 \leqslant t_{00} \leqslant 4$. This leaves four cases to consider.

$\mathbf{t_{00} = 0}$: If $t_{00} = 0$, it is forced by (8.1) that t_{01} is at least 3. Then it follows from Lemma 52 and (8.4) that $t_{01} = 3$. Lemma 48 and (8.4) can be applied to show that $t_{11} = 0$ and because of (8.2) it follows that $t_{10} \geqslant 3$. At the same time, Conclusion 2 forces t_{10} to be at most 4. Hence, $t_{21} \geqslant 1$, because of (8.3), which contradicts Conclusion 6. Therefore, this case cannot occur.

$\mathbf{t_{00} = 1}$: One can apply (8.1) to show that $t_{01} \geqslant 2$. This, together with Lemma 52, reveals that $2 \leqslant t_{01} \leqslant 3$. Again, Lemma 48 forces t_{11} to be zero. Because of (8.2) it follows that t_{10} is at least 2 and, by Conclusion 2, at most 4. Lemma 51 coerces t_{01} to be 2 and hence (8.3) makes it necessary for t_{21} to be at least 1. Conclusion 6 can be applied to obtain $t_{10} = 2$, which leads together with (8.3) to $t_{21} \geqslant 3$. This contradicts Conclusion 4 and therefore t_{00} cannot be smaller than 2.

$\mathbf{t_{00} = 2}$: For $t_{00} = 2$, it follows that $1 \leqslant t_{01} \leqslant 3$ because of (8.1) and Lemma 52. Hence, (8.2) can be applied to show that $v_1 \geqslant 1$. At this point, further restrictions do not follow from the lemmata above, hence another case analysis is necessary.

- $\mathbf{t_{01} = 3}$: Lemmata 48 and 51 restrict t_{11} to be 0 and t_{10} to be at most 1. But then one has $t_{10} = v_1$ which has to be at least 1, as proven above. Hence, $t_{10} = 1$ follows. Then t_{21} needs to be at least 2 because of (8.3), which contradicts Conclusion 4.
- $\mathbf{t_{01} = 2}$: Again, Lemma 48 shows that $t_{11} = 0$. But here, (8.2) displays that $2 \leqslant v_1 = t_{10}$, which contradicts Lemma 55.
- $\mathbf{t_{01} = 1}$: Here, (8.2) can be applied to show that v_1 is at least 3 and Conclusion 2 to obtain $t_{10} \leqslant 4$. Unfortunately, this is not enough to conclude anything else and another case analysis is in order.
    - $\mathbf{t_{10} \geqslant 3}$: It follows from Conclusion 6 that $t_{21} = 0$ and hence from (8.3) that $v_1 \geqslant 5$. Hence, $t_{11} \geqslant 1$ which contradicts Lemma 53.
    - $\mathbf{t_{10} = 2}$: By (8.2) it follows that t_{11} is at least 1, which contradicts Lemma 53.

$\mathbf{t_{10} = 1}$: It follows from (8.2) and Conclusion 9 that t_{11} has to be at least 2 and at most 3. This leads, with (8.3) which shows that $t_{21} \geqslant 1$, to a contradiction with Conclusion 7.

$\mathbf{t_{10} = 0}$: Here, t_{11} is greater than 3 because of (8.2). Conclusion 5 can be applied to show that $t_{21} = 0$ and hence $t_{11} \geqslant 5$ follows by (8.3) which contradicts with Conclusion 3.

Every case with $t_{00} = 2$ and $t_{01} = 1$ leads to a contradiction, hence a conditioned system (4.1) with $s \geqslant 8$ and these two parameters has a non-trivial 3-adic solution.

This proves for the last possible value of t_{01} if $t_{00} = 2$ that there exist a non-trivial 3-adic solution, hence $t_{00} = 2$ cannot occur if such a solution does not exist.

$\mathbf{t_{00} = 3}$: It follows from Lemmata 47 and 49 that $t_{11} = 0$ and $t_{01} \leqslant 1$. Hence, Conclusion 2 and (8.2) forces t_{10} to be at least 2 and at most 4. By Conclusion 4, it follows that $t_{21} \leqslant 1$ and hence, due to (8.3) one obtains $3 \leqslant t_{10} \leqslant 4$. Conclusion 6 shows that $t_{21} = 0$ and hence, again due to (8.3), $t_{01} = 1$, which contradicts Lemma 54.

$\mathbf{t_{00} = 4}$: Again one sees with Lemmata 47 and 49 that $t_{11} = 0$ and $t_{01} \leqslant 1$. Hence, by (8.2), the parameter t_{10} is at least 1 which contradicts Lemma 50.

As shown above, a conditioned system (4.1) with $s \geqslant 8$ which has no non-trivial 3-adic solution cannot have $t_{00} \leqslant 4$. But as proven before the case analysis those cases with $t_{00} \geqslant 5$ do have a non-trivial 3-adic solution, hence the lemma is proven. □

As discussed at the beginning of this section, this suffices to prove Theorem 1 for $p = 3$. For every other prime the theorem was proven in the previous section, hence Theorem 1 holds.

Acknowledgement. I want to express my sincere gratitude to Prof. Jörg Brüdern who gave me the initial introduction to the problem and supported me on my way to solve it.

References

1. E. Artin, *The Collected Papers of Emil Artin*, Addison-Wesley (Reading, MA, 1965).
2. J. Brüdern and O. Robert, On Artin's conjecture: linear slices of diagonal hypersurfaces. *Trans. Amer. Math. Soc.* **372**(3) (2019), 1867–1911.
3. S. Chowla, H. B. Mann and E. G. Straus, Some applications of the Cauchy-Davenport theorem. *Norske Vid. Selsk. Forh. Trondheim* **32** (1959), 74–80.
4. H. Davenport and D. J. Lewis, Homogeneous additive equations. *Proc. Roy. Soc. Ser. A* **274** (1963), 443–460.
5. M. Dodson, Homogeneous additive congruences. *Philos. Trans. Roy. Soc. London Ser. A* **261** (1967), 163–210.
6. D. B. Leep and C. C. Yeomans, The number of points on a singular curve over a finite field. *Arch. Math.* (*Basel*) **63**(5) (1994), 420–426.
7. D. J. Lewis, Cubic homogeneous polynomials over p-adic number fields. *Ann. of Math.* (2) **56** (1952), 473–478.
8. D. J. Lewis, Cubic congruences. *Michigan Math. J.* **4** (1957), 85–95.
9. L. J. Mordell, A remark on indeterminate equations in several variables. *J. Lond. Math. Soc.* **s1-12**(1), 127.
10. W. M. Schmidt, *Equations over Finite Fields An Elementary Approach*, Springer (Berlin, 1976).

Miriam Sophie Kaesberg,
Mathematisches Institut,
Georg-August-Universität Göttingen,
D-37073, Göttingen,
Germany
Email: miriam.kaesberg@mathematik.uni-goettingen.de

Mathematika is owned by University College London and published by the London Mathematical Society. All surplus income from the publication of *Mathematika* is returned to mathematicians and mathematics research via the Society's research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.