Two Cases of Artin's Conjecture

Dissertation

for the award of the degree

"Doctor rerum naturalium"

of the Georg-August-Universität Göttingen

within the doctoral program "Mathematical Sciences"

of the Georg-August University School of Science (GAUSS)

submitted by

Miriam Sophie Kaesberg

from Rinteln

Göttingen, 2020

Thesis committee

Prof. Dr. Jörg Brüdern,
Mathematisches Institut, Georg-August-Universität Göttingen

Prof. Dr. Preda Mihăilescu,
Mathematisches Institut, Georg-August-Universität Göttingen

Members of the Examination Board

Reviewer:
Prof. Dr. Jörg Brüdern,
Mathematisches Institut, Georg-August-Universität Göttingen

Second Reviewer:
Prof. Dr. Preda Mihăilescu,
Mathematisches Institut, Georg-August-Universität Göttingen

Further members of the Examination Board

Prof. Dr. Damaris Schindler,
Mathematisches Institut, Georg-August-Universität Göttingen

Prof. Dr. Dorothea Bahns,
Mathematisches Institut, Georg-August-Universität Göttingen

Prof. Dr. Gerlind Plonka-Hoch,
Institut für Numerische und Angewandte Mathematik, Georg-August-Universität Göttingen

Prof. Dr. Anja Sturm,
Institut für Mathematische Stochastik, Georg-August-Universtität Göttingen

Date of the oral examination: December 18, 2020

Contents

1 Introduction

A conjecture by Emil Artin [2] states that a form f (homogeneous polynomial) of degree k with integer coefficients in s variables has a non-trivial solution of $f = 0$ in $\mathbb{Q}_p$ for all primes p if $s > k^2$. A non-trivial solution of the form f is a solution $f(\boldsymbol{x}) = 0$ with at least one $x_i \neq 0$. The only cases in which this conjecture is known to be true are the ones with $k = 1$, which is trivial, $k = 2$ by Meyer [33] and $k = 3$ by Dem'yanov [15] for $p \neq 3$ and, independently, by Lewis [29] for all primes p. But in general the conjecture was disproved by Terjanian [39] with a counterexample in the case $k = 4$. He used the quartic form

$$g(x, y, z) = xyz\,(x + y + z) + x^2y^2 + x^2z^2 + y^2z^2 - x^4 - y^4 - z^4$$

in three variables to compose a quartic form

$$\begin{aligned} f(x_1, \ldots, x_{18}) = {} & g(x_1, x_2, x_3) + g(x_4, x_5, x_6) + g(x_7, x_8, x_9) \\ & + 4g(x_{10}, x_{11}, x_{12}) + 4g(x_{13}, x_{14}, x_{15}) + 4g(x_{16}, x_{17}, x_{18}) \end{aligned}$$

in $18 > 4^2$ variables and proved that the equation $f(\boldsymbol{x}) = 0$ has only the trivial solution in $\mathbb{Q}_2$. Browkin [4] even found for all primes p forms f of some degree k in more than k^2 variables without a non-trivial p-adic solution of the equation $f = 0$. However, none of these was a form in more than k^3 variables, leaving the possibility that Artin's conjecture could be true provided that $s > k^3$ or at least $s > k^n$ for some $n \in \mathbb{N}$. Results by Arkhipov and Karatsuba [1], Brownawell [6], and Lewis and Montgomery [31] showed that this hope was in vain. For every $n \in \mathbb{N}$ and every prime they found infinitely many degrees k for which there are counterexamples in more than k^n variables.

Nonetheless, there are different directions in which one can still examine Artin's conjecture. One of them is indicated by a similarity between all known counterexamples. They all disprove Artin's conjecture for an even degree. Thus, Artin's conjecture could still hold for forms of odd degree or, maybe more likely, for forms of prime degree.

Another direction was pursued by Ax and Kochen [3] who proved for all degrees k that there are only finitely many primes p for each k such that there are forms f of degree k in $s > k^2$ variables for which the equation $f(x) = 0$ does not have a non-trivial solution in $\mathbb{Q}_p$. In particular, for every k there is a number $p_0(k)$ such that for all forms f of degree k in $s > k^2$ variables the equation $f(x) = 0$ has a non-trivial p-adic solution for all $p > p_0(k)$. Furthermore, they could prove a generalisation of this statement. Namely, that for every R-tuple $(k_1, \ldots, k_R) \in \mathbb{N}^R$ there is a finite set of primes $A = A(k_1, \ldots, k_R)$ such that for all primes $p \notin A$ and every system $f_1, \ldots, f_R$, where f_i is a form in s variables of degree k_i for $1 \leq i \leq R$, the equations $f_1 = \cdots = f_R = 0$ have a non-trivial p-adic solution provided that $s > k_1^2 + \cdots + k_R^2$. Again, it follows directly that there is a natural number $p_1(k_1, \ldots, k_R)$ such that for all primes $p > p_1(k_1, \ldots, k_R)$ the equations $f_1 = \cdots = f_R = 0$ have a non-trivial p-adic solutions for all forms f_i of degree k_i. However, their work does not give an explicit bound for $p_0(k)$ and $p_1(k_1, \ldots, k_R)$. While there are explicit bounds for $p_0(k)$ and $p_1(k_1, \ldots, k_R)$ (see

Brown [5] and Cohen [11]), these bounds contain nested exponentials and are, therefore, huge. For some small values of k there are better bounds for $p_0(k)$ known, for example, $p_0(5) \leq 7$ by Dumke [18] and both $p_0(7) \leq 883$ and $p_0(11) \leq 8053$ by Wooley [43].

A different approach is to restrict the forms instead of the primes. A popular way is to focus on diagonal forms, for which Davenport and Lewis [12] have proved Artin's conjecture. Thereby, a diagonal form

$$f(x_1, \ldots, x_s) = \sum_{i=1}^{s} a_i x_i^k$$

has a non-trivial p-adic solution for all primes p provided that $s > k^2$.

A generalisation of Artin's conjecture for diagonal forms to systems of R diagonal forms of degree $k_1, \ldots, k_R$ leads to the following question. Do the equations $f_1 = \cdots = f_R = 0$ for the forms

$$f_j(x_1, \ldots, x_s) = \sum_{i=1}^{s} a_{ij} x_i^{k_j} \quad (1 \leq j \leq R)$$

have a non-trivial p-adic solution provided that $s > k_1^2 + \cdots + k_R^2$?

For this version of Artin's conjecture, it is known, due to the result on R forms by Ax and Kochen [3] mentioned earlier, that the conjecture holds for each R-tuple $(k_1, \ldots, k_R)$ for all but a finite set of primes. But in general, it follows from a result by Lewis and Montgomery [31, Theorem 2] that this conjecture is not true and, furthermore, Wooley [42] proved that even the case $R = 2$ does not hold for all tuples (k_1, k_2). However, there are cases in which it does hold. For example, the case $(k_1, k_2) = (3, 2)$ was proved by Wooley [41] and $(k_1, k_2) = (k, 1)$ for general k by Brüdern and Robert [9].

The case $k := k_1 = k_2 = \cdots = k_R$ was first examined by Davenport and Lewis [13] who proved that such a system of equations has a non-trivial p-adic solution if

$$s \geq 2R^2 k \log k \text{ (for k odd)} \quad \text{or} \quad s \geq 48R^2k^3 \log\left(3Rk^2\right) \text{ (for } k > 2)$$

holds. Brüdern and Godinho [7] improved this for $k \geq 3$ and $R \geq 3$ to

$$s \geq R^3 k^2,$$

unless one has $R = 3$ and $k = 2^\tau$ for some $\tau \geq 1$, in which case $s \geq 36k^2$ suffices. This was the first bound for the case $k_1 = \cdots = k_R = k$ with the expected order of magnitude k^2. Later, Knapp [25] was able to improve this bound to $s \geq 4R^2k^2$ for all $R \in \mathbb{N}$ and $k \geq 2$.

Further research was done on the case $R = 2$. Davenport and Lewis [14] proved that the expected bound $s > 2k^2$ holds if k is odd, whereas for even k they only obtained the bound $s \geq 7k^3$. Brüdern and Godinho [8] have proved that the expected bound $s > 2k^2$ holds for even k which are not of the shape

$$k = 3 \cdot 2^\tau \quad \text{or} \quad k = p^\tau (p-1)$$

for p prime and $\tau \geq 1$ as well. For each of these excluded shapes they proved for all but one prime that a non-trivial p-adic solution exists if $s > 2k^2$. The missing primes are $p = 2$ in the case $k = 3 \cdot 2^\tau$ and p if $k = p^\tau (p-1)$. Here, they gave the bounds $s \geq \frac{8}{3}k^2$ for $p = 2$ and $k = 3 \cdot 2^\tau$,

$s \geq 8k^2$ for $p = 2$ and $k = 2^\tau$, and $s \geq 4k^2$ for $p \geq 3$ and $k = p^\tau (p-1)$. All in all, this established the bound $s \geq 8k^2$ for all p and all k.

There was some further progress for $p = 2$ and $k = 2^\tau$ for $\tau = 1$, $\tau = 2$ and $\tau \geq 16$. For $k = 2$ the expected bound $s > 8$ follows from the general result by Dem'yanov [16] that for two quadratic forms f_1, f_2 in at least nine variables the equations $f_1 = f_2 = 0$ have a non-trivial p-adic solution for all primes p. Poehler [37] proved for $k = 4$ that $49 = 3k^2 + 1$ variables suffice and Kränzlein [26] showed for $k = 2^\tau$ with $\tau \geq 16$ that the expected $2k^2 + 1$ variables are sufficient.

For $p \geq 3$ and $k = p^\tau (p-1)$ on the other hand, the bound was further sharpened by Godinho and de Souza Neto [20, 21] who proved that

$$s > 2\frac{p}{p-1}k^2 - 2k$$

suffices for $p \in \{3, 5\}$ and if $\tau \geq \frac{p-1}{2}$ for $p \geq 7$ as well. Campos Vargas [40] announced the same bound in the cases $\tau \geq 3$ provided that $p \geq 7$ and for $\tau = 2$ if $p \geq \frac{C}{2} + 4$, where $C \geq 3$ is a constant satisfying certain conditions for which he can show that one has $C \leq 9997$. Furthermore, for $\tau = 1$, it was announced by him that $s > \left(2\frac{p}{p-1} + \frac{C-3}{2p-2}\right)k^2 - 2k$ variables are sufficient for $p \geq 5$. Due to the connection $k = p^\tau (p-1)$ between k and p, one can easily see that the bound $2\frac{p}{p-1}k^2 - 2k$ is worse than Artin's bound $2k^2 + 1$ in every case. Nonetheless, by combining these results, he proved that for every $\varepsilon > 0$ the bound $s > (2 + \varepsilon)k^2$ is sufficient for p large enough.

For $k = 6 = 3 \cdot 2$, the bound $s > 2k^2$ was reached by Godinho, Knapp and Rodrigues [22] while later Godinho and Ventura [23] showed that this bound suffices for $k = 3^\tau \cdot 2$ with $\tau \geq 2$ as well. Therefore, all pairs of diagonal forms of equal degree k in more than $2k^2$ variables have a non-trivial 3-adic solution. Chapter 2, which contains the proof of the following theorem, shows that this statement does not only hold for $p = 3$ but for all $p \geq 3$, by taking care of the degrees $k = p^\tau (p-1)$ for $p \geq 5$ and $\tau \geq 1$.

Theorem 1. *Let $p \geq 5$ be a prime, $\tau \geq 1$ and $k = p^\tau (p-1)$. Then for $a_i, b_i \in \mathbb{Z}$ with $1 \leq i \leq s$, the equations*

$$\sum_{i=1}^{s} a_i x_i^k = \sum_{i=1}^{s} b_i x_i^k = 0 \tag{1.0.1}$$

have a non-trivial p-adic solution for all $s > 2k^2$.

This completes the proof of Artin's conjecture for two diagonal forms of equal degree for all odd primes. For $p = 2$ there are only the questions left whether there is a non-trivial 2-adic solution for $k = 3 \cdot 2^\tau$ for $\tau \geq 2$ and $k = 2^\tau$ for $2 \leq \tau \leq 15$ provided that $s > 2k^2$. The argument by Kränzlein [26] can be easily applied for the case $k = 3 \cdot 2^\tau$ as well if $\tau \geq 16$. Thus, only finitely many k remain for which the bound $s > 2k^2$ is not reached.

The proof of Theorem 1 follows a pattern by Davenport and Lewis [14] while making use of some improvements by Brüdern and Godinho [8]. Section 2.1 defines an equivalence relation on the set of all systems (1.0.1), introduced by Davenport and Lewis [14]. This equivalence relation is defined in a way that solubility of (1.0.1) in $\mathbb{Q}_p^s \backslash \{\mathbf{0}\}$ is preserved, which allows to pick representatives with useful properties from each class and prove the existence of a non-trivial p-adic solution only for them. Due to a version of Hensel's lemma, one can show

that a system (1.0.1) has a non-trivial p-adic solution by proving that the congruences

$$\sum_{i=1}^{s} a_i x_i^k \equiv \sum_{i=1}^{s} b_i x_i^k \equiv 0 \mod p^{\tau+1} \tag{1.0.2}$$

have a solution for which the matrix

$$\begin{pmatrix} a_1x_1 & a_2x_2 & \dots & a_sx_s \\ b_1x_1 & b_2x_2 & \dots & b_sx_s \end{pmatrix} \tag{1.0.3}$$

has rank 2 modulo p. Section 2.2 recalls the notions of coloured variables, introduced by Brüdern and Godinho [8], and contractions which were established by Davenport and Lewis [14]. Together, they are the foundation of the proof. Coloured variables and a refinement of them provide a way to take care of the rank of the matrix (1.0.3), while contractions are a means to solve the equations (1.0.2) recursively by lifting solutions modulo p^l to solutions modulo p^{l+1}. Furthermore, this section continues the path laid down by Davenport and Lewis [14] and Brüdern and Godinho [8], which issues more restrictions on the pairs of equations one has to find a solution for. Section 2.3 is a collection of combinatorial results which are frequently used, directly and indirectly, in the remaining sections. A description on how the notion of coloured variables is used in combination with contractions to obtain a solution of (1.0.2) such that the matrix (1.0.3) has rank 2 is contained in Section 2.4, whereas Section 2.5 consists of a collection of lemmata which describe situations in which one can lift some solutions modulo p^l to solutions of a higher modulus. The remaining two sections contain the actual proof which is divided into Section 2.6 for the case $k = p(p-1)$ and Section 2.7, where the remaining cases with $k = p^\tau(p-1)$ and $\tau \geq 2$ are handled. This division is due to the different modulus in (1.0.2). For big τ, one has more variables whose coefficients are not both congruent to 0 modulo $p^{\tau+1}$, which is balanced in the case $\tau = 1$ by a permutation argument.

The cases $R \in \mathbb{N}$ with $k_1 = k$ and $k_2 = \dots = k_R = 1$ of the generalisation of Artin's conjecture for diagonal forms merit particular attention. As Brüdern and Robert [9] pointed out, they could be used as a means to prove Artin's conjecture for some k. The following lemma [9, Section 2], an immediate conclusion of a theorem by Ellison [19], which works over $\mathbb{Q}_p$ as well, describes why this is the case, and which values of R are important for that.

Lemma 1. *For a form $g \in \mathbb{Q}[X_1, \dots, X_s]$ of degree k there are r forms $L_j \in \mathbb{Q}[Y_1, \dots, Y_{r+s}]$ $(1 \leq j \leq r)$ of degree 1 and $r+s$ coefficients $c_j \in \mathbb{Q}$ $(1 \leq j \leq r+s)$ for*

$$0 \leq r \leq \frac{s(s+1)\dots(s+k-1)}{k!}$$

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

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

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

Consequently, Artin's conjecture for systems of diagonal forms containing one form of

degree k and r linear forms for all

$$0 \leq r \leq \frac{\left(k^2+1\right)\left(k^2+2\right)\cdots\left(k^2+k\right)}{k!}$$

implies Artin's conjecture for forms of degree k.

Leep and Schmidt [27] claimed that if for all systems $f_1, \ldots, f_R$ of R diagonal forms of degree $k_1, \ldots, k_R$ in s variables there is a non-trivial p-adic solution of the equations $f_1 = \cdots = f_R = 0$, then the same holds for $R+r$ diagonal forms of degree $k_1, \ldots, k_R, 1, \ldots, 1$ in $s+r$ variables. It is easy to see that this statement holds for general forms. There, one can transform a system of R forms of degree $k_1, \ldots, k_R$ and r linear forms in $s+r$ variables into R forms of degree $k_1, \ldots, k_R$ in s variables just by plugging the linear forms into the R forms of degree $k_1, \ldots, k_R$. However, for diagonal forms one encounters the problem that the resulting system of forms of degree $k_1, \ldots, k_R$ is not necessarily diagonal as well. Furthermore, it turns out to be wrong for diagonal forms, because this would imply Artin's conjecture when combined with Lemma 1 and the result by Davenport and Lewis [12] for one diagonal form. As Artin's conjecture does not hold in general, this leads to a contradiction and the case $(k, 1, \ldots, 1)$ remains an open problem.

For $r = 0$, this is the case of one diagonal form which was proved by Davenport and Lewis [12] as mentioned before. Brüdern and Robert [9] took care of the case $r = 1$ by proving that $s > k^2 + 1$ variables suffice to ensure the existence of a non-trivial p-adic solution for all primes. Nonetheless, the condition $s > k^2 + r$ cannot be sufficient for all $r \in \mathbb{N}$, because this would prove Artin's conjecture for all k, but it would be of interest to know up to which r this is true.

In the case $k = 3$ Artin's conjecture holds. It follows that for every system containing one form f_1 of degree 3 and r linear forms $f_2, \ldots, f_{r+1}$ in s variables the equations $f_1 = f_2 = \cdots = f_{r+1} = 0$ have a non-trivial p-adic solution for all primes p provided that $s \geq 10 + r$. This can be seen by plugging in the linear equations in the cubic equation, which resolves in a cubic form in at least ten variables which is solvable. In general, Artin's conjecture is strict for $k = 3$, which Mordell [34] proved. Therefore, there are cubic forms in nine variables which do not have a solution for all primes p. Naturally, this is not true for all cubic forms in nine variables. To examine this, one can subdivide the set of cubic forms in s variables based on the related parameter

$$r \in \left\{0, 1, \ldots, \frac{s\,(s+1)\,(s+2)}{6}\right\}$$

as implied by Lemma 1 and ask the question how many variables are necessary for cubic forms with a fixed parameter r.

The case $r = 0$ was tackled by Lewis [30]. He 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 provided that $s \geq 7$, and, therefore, that all cubic forms with $r = 0$ have a non-trivial p-adic solution for all p if $s \geq 7$. Furthermore, he even proved that there is a diagonal cubic form in six variables without a non-trivial p-adic solution for some prime p. Thus, the bound is best possible. It improves upon the bound obtained through Artin's conjecture by three variables.

The aim of Chapter 3 is to prove that for cubic forms with $r = 1$ one does not loose this advantage of three variables, which is an immediate conclusion of the following theorem.

Theorem 2. *Let $s \geq 8$ and $a_i, b_i \in \mathbb{Z}$ for $1 \leq i \leq s$. Then the system*

$$\sum_{j=1}^{s} a_j x_j^3 = \sum_{j=1}^{s} b_j x_j = 0, \tag{1.0.4}$$

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

If this statement were correct for $s \geq 7$ as well, it would follow by taking, for example, $b_1 = 1$ and $b_i = 0$ for $2 \leq i \leq s$ that all diagonal cubic equations in at least six variables have a non-trivial p-adic solution for all primes p, which contradicts Lewis [30] result that the bound $s \geq 7$ is strict for cubic diagonal forms. Thus, this is the best possible bound for s.

Likewise, it is impossible for all systems

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

with integer coefficients a_j and b_{ij} to have a non-trivial p-adic solution for all primes p and all $0 \leq r \leq 84 = \frac{7 \cdot 8 \cdot 9}{6}$. 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, which contradicts that the bound from Artin's conjecture is strict for $k = 3$. Hence, somewhere between $r = 2$ and $r = 220 = \frac{10 \cdot 11 \cdot 12}{6}$ this gap of three variables have to close itself.

The proof of Theorem 2 follows a pattern by Brüdern and Robert [9]. The difficulty of finding a non-trivial p-adic solution for all systems of equations (1.0.4) depends on the residue class of p modulo 3. Those primes congruent to 2 modulo 3 are treated in Section 3.1 with a contraction argument by Brüdern and Robert [9, Section 3], which traces the problem of finding a non-trivial p-adic solution of (1.0.4) back to the equation

$$c_1 x_1^3 + \cdots + c_t x_t^3 = 0 \tag{1.0.5}$$

and the question which $t \in \mathbb{N}$ guarantee the solubility in $\mathbb{Q}_p$. For p congruent to 2 modulo 3 a solution of (1.0.5) exists for relatively small t in comparison to primes p congruent to 1 modulo 3 due to Dodson [17]. For the remaining primes, the version of Hensel's lemma in Section 3.2 established by Brüdern and Robert [9, Section 4], gives a combinatorial approach to the problem. If the system of congruences

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

with $\gamma = 1$ for $p \neq 3$ and $\gamma = 2$ for $p = 3$ has a solution in the integers such that there are $i, j \in \{1, \ldots, s\}$ with

$$p \nmid b_i a_j x_j^2 - b_j a_i x_i^2,$$

there is a non-trivial p-adic solution of the equations (1.0.4) as well. This indicates a necessity to distinguish between primes congruent to 1 modulo 3 and the prime 3. An equivalence

relation on the set of systems (1.0.4) which preserves the solubility in $\mathbb{Q}_p^s \backslash \{\mathbf{0}\}$, introduced by Brüdern and Robert [9, Section 6], is used in Section 3.3 to pick representatives with useful properties to fulfil the requirements of the version of Hensel's lemma. Most cases for p congruent to 1 modulo 3 can be worked on with a simple combinatorial approach in Section 3.4, where one finds a solution using only the variables whose coefficients a_i and b_i are not both divisible by p. This leaves three cases which require more attention.

The first of those is treated in Section 3.5 using a more complex, but still combinatorial, approach of Brüdern and Robert [9, Sections 8 and 9], which does not only focus on those variables whose coefficients a_i and b_i are not both divisible by p but on all, and a result by Leep and Yeomans [28] on the number of solutions of an absolutely irreducible polynomial. The two remaining cases can be solved, again using only the variables whose coefficients a_i and b_i are not both divisible by p, by Leep and Yeomans result as in the first case. This reduces the problem to proving that some specific polynomials are absolutely irreducible, which is either done by contradiction or by using a result by Schmidt [38]. This leaves only the case $p = 3$, which is solved solely combinatorially in Section 3.7.

2 Pairs of Diagonal Forms

This chapter contains the proof of the following theorem, which claims that for two diagonal forms f, g of degree $k = p^\tau (p-1)$ for $p \geq 5$ and $\tau \geq 1$ in s variables the equations $f = g = 0$ have a non-trivial p-adic solution provided that $s > 2k^2$.

Theorem 1. *Let $p \geq 5$ be a prime, $\tau \geq 1$ and $k = p^\tau (p-1)$. Then for $a_i, b_i \in \mathbb{Z}$ with $1 \leq i \leq s$, the equations*

$$\sum_{i=1}^{s} a_i x_i^k = \sum_{i=1}^{s} b_i x_i^k = 0 \tag{1.0.1}$$

have a non-trivial p-adic solution for all $s > 2k^2$.

Even though it would suffice to focus on the case $k = p^\tau (p-1)$ and $p \geq 5$, Sections 2.1, 2.2 and 2.3 hold in the general case, where k is a natural number and p any prime as well.

2.1 p-Normalisation

This section recalls an equivalence relation on the set of systems (1.0.1) which was introduced by Davenport and Lewis [14] in order to choose representatives with specific characteristics.

Define for any pair of diagonal forms

$$f = \sum_{i=1}^{s} a_i x_i^k, \qquad g = \sum_{i=1}^{s} b_i x_i^k \tag{2.1.1}$$

with rational coefficients a_i and b_i $(1 \leq i \leq s)$ a rational number

$$\vartheta(f, g) := \prod_{\substack{1 \leq i,j \leq s \\ i \neq j}} (a_i b_j - a_j b_i).$$

For integers ν_i $(1 \leq i \leq s)$ consider the pair

$$f' = f(p^{\nu_1} x_1, \ldots, p^{\nu_s} x_s), \qquad g' = g(p^{\nu_1} x_1, \ldots, p^{\nu_s} x_s) \tag{2.1.2}$$

and for rational numbers λ_1, λ_2, μ_1 and μ_2 with $\lambda_1 \mu_2 - \lambda_2 \mu_1 \neq 0$ the pair

$$f'' = \lambda_1 f + \lambda_2 g, \qquad g'' = \mu_1 f + \mu_2 g. \tag{2.1.3}$$

If another pair $\tilde{f}, \tilde{g}$ with rational coefficients can be obtained by a finite succession of the operations (2.1.2) and (2.1.3) on the pair f, g, then they are called p-equivalent. If $(x_1', \ldots, x_s')$ is a non-trivial solution of $f' = g' = 0$ then $(p^{\nu_1} x_1', \ldots, p^{\nu_s} x_s')$ is a non-trivial solution of $f = g = 0$, whereas if $(x_1, \ldots, x_s)$ is a non-trivial solution for $f = g = 0$, then one has a non-trivial solution for $f' = g' = 0$ as well, given via $(p^{-\nu_1} x_1, \ldots, p^{-\nu_s} x_s)$. Therefore, solubility is preserved under

the operation (2.1.2). The same holds for the operation (2.1.3). Here, one direction is obvious, and the other holds, because the transformation is invertible. Consequently, the existence of a non-trivial solution for $f = g = 0$ in $\mathbb{Q}_p$ implies that there is one for all pairs $\tilde{f}, \tilde{g}$ which are p-equivalent to f, g. It can also be easily deduced from the definition of $\vartheta(f, g)$ that if $\vartheta(f, g) = 0$, the same holds for $\vartheta(f', g')$ and $\vartheta(f'', g'')$ and, therefore, for the whole p-equivalence class.

Definition 1. A pair f, g given by (2.1.1) with integers coefficients and $\vartheta(f, g) \neq 0$ is called *p-normalised*, if the power of p dividing $\vartheta(f, g)$ is as small as possible amongst all pairs of forms (2.1.1) with integer coefficients in the same p-equivalence class.

As each p-equivalence class contains pairs for which all coefficients a_i, b_i are integers, it follows that the existence of a non-trivial solution for all p-normalised pairs induces a non-trivial solution for all pairs of forms with rational coefficients a_j, b_j and $\vartheta(f, g) \neq 0$. Using a compactness argument, Davenport and Lewis [14] showed that it induces the existence of a solution for all pairs of forms f, g with $\vartheta(f, g) = 0$ as well.

Lemma 2. *Suppose for a fixed s that the equations $f = g = 0$ have a non-trivial solution in $\mathbb{Q}_p$ for all p-normalised pairs f, g. Then, for any rational coefficients a_j, b_j, the equations* (1.0.1) *have a non-trivial solution in $\mathbb{Q}_p$.*

Proof. See [14, Section 5]. □

Consequently, it suffices to focus on finding non-trivial p-adic solutions for p-normalised pairs f, g in more than $2k^2$ variables. The following lemma gives information about the properties of them.

Lemma 3. *A p-normalised pair of diagonal forms f, g of degree k in s variables can be written as*

$$f = f_0 + pf_1 + \cdots + p^{k-1} f_{k-1},$$
$$g = g_0 + pg_1 + \cdots + p^{k-1} g_{k-1},$$

where f_i, g_i are forms in m_i variables, and these sets of variables are disjoint for $i = 0, 1, \ldots, k-1$. Moreover, each of the m_i variables occurs in at least one of f_i, g_i with a coefficient not divisible by p. One has

$$m_0 + \cdots + m_j \geq \frac{(j+1)\, s}{k} \qquad \text{for} \qquad j = 0, 1, \ldots, k-1. \tag{2.1.4}$$

Moreover, if q_i denotes the minimum number of variables appearing in any form $\lambda f_i + \mu g_i$ (λ and μ not both divisible by p) with coefficients not divisible by p, then

$$m_0 + \cdots + m_{j-1} + q_j \geq \frac{\left(j + \frac{1}{2}\right) s}{k} \qquad \text{for} \qquad j = 0, 1, \ldots, k-1.$$

Proof. See [14, Lemma 9]. □

At least one integer coefficient a_i or b_i of a variable x_i of a p-normalised pair f, g is non-zero, because else one would have $\vartheta(f, g) = 0$. Consequently, there is a maximal power l of p, which divides both a_i and b_i. Due to the previous lemma, one can deduce that $0 \leq l \leq k-1$ for all variables x_i of a p-normalised pair.

Definition 2. A variable x_i of a pair f, g with integer coefficients is said to be *at level* l if its coefficients a_i and b_i are both divisible by p^l but not both divisible by p^{l+1}.

By Lemma 3, a p-normalised pair has exactly m_l variables at level l for $0 \le l \le k-1$. The integers $\tilde{a}_i, \tilde{b}_i$ are defined for a variable x_i at level l with integer coefficients a_i, b_i via $\tilde{a}_i = p^{-l} a_i$ and $\tilde{b}_i = p^{-l} b_i$. These integers $\tilde{a}_i, \tilde{b}_i$ are the coefficients of the forms f_l, g_l as defined in Lemma 3 and the vector $\binom{\tilde{a}_i}{\tilde{b}_i}$ is called the *level coefficient vector* of a variable x_i.

One can restrict the question of the existence of a non-trivial p-adic solution to one of congruences. To this end, it is useful to adopt the notation $k = p^\tau \delta k_0$ with $\delta = \gcd(k, p-1)$, $\gcd(p, k_0) = 1$ and

$$\gamma := \begin{cases} 1, & \text{if } \tau = 0 \\ \tau + 1, & \text{if } \tau > 0 \text{ and } p > 2 \\ \tau + 2, & \text{if } \tau > 0 \text{ and } p = 2, \end{cases} \tag{2.1.5}$$

by Davenport and Lewis [14] which is used in the following lemma.

Lemma 4. *If the congruences*

$$\sum_{i=1}^{s} a_i x_i^k \equiv 0 \mod p^\gamma, \qquad \sum_{i=1}^{s} b_i x_i^k \equiv 0 \mod p^\gamma \tag{2.1.6}$$

have a solution in the integers for which the matrix

$$\begin{pmatrix} a_1 x_1 & a_2 x_2 & \dots & a_s x_s \\ b_1 x_1 & b_2 x_2 & \dots & b_s x_s \end{pmatrix}$$

has rank 2 *modulo* p*, then the equations* (1.0.1) *have a non-trivial* p*-adic solution.*

Proof. See [14, Lemma 7]. □

Such a solution is called a *non-singular solution*. The remainder of this chapter focuses on finding non-singular solutions for p-normalised pairs f, g.

The next section introduces the methods used to find non-singular solutions.

2.2 Coloured Variables and Contractions

This section recalls the concept of coloured variables, first used by Brüdern and Godinho [8], and refine it in a way such that it meets the requirements of the special case $k = p^\tau (p-1)$. It also describes the method of contractions which was introduced by Davenport and Lewis [14]. Together, both concepts form the foundation of this proof.

To have more control over the non-singularity of a solution of (2.1.6), Brüdern and Godinho [8] divided the set of variables at level l into $p+1$ sets, depending on their level coefficient vector. For that, they defined the vectors $\boldsymbol{e}_0 = \binom{1}{0}$ and $\boldsymbol{e}_\nu = \binom{\nu}{1}$ for $\nu \in \{1, \dots, p\}$. Viewed as vectors in $(\mathbb{Z}/p\mathbb{Z})^2$ the vectors define the sets

$$\mathscr{L}_\nu := \left\{ c\boldsymbol{e}_\nu \mid c \in (\mathbb{Z}/p\mathbb{Z})^* \right\}$$

for $0 \le \nu \le p$. Modulo p, each level coefficient vector $\left(\tilde{a}_i, \tilde{b}_i\right)$ lies in exactly one of the disjoint sets $\mathscr{L}_\nu$.

Definition 3. A variable x_i at level l is said to be of *colour* ν, if the level coefficient vector $\left(\tilde{a}_i, \tilde{b}_i\right)$ interpreted as a vector in $\mathbb{F}_p^2$ lies in $\mathscr{L}_\nu$. The parameter I_ν^l of a pair f, g is the number of variables x_i at level l of colour ν.

The parameter q_l introduced in Lemma 3 denotes the minimum number of variables appearing with a coefficient not divisible by p in any form $\lambda f_l + \mu g_l$ with $(\lambda, \mu) \not\equiv (0,0)$ modulo p. This is closely related to the concept of coloured variables. By setting $\lambda \equiv 0$ modulo p for $\nu = 0$ or $\mu \equiv -\lambda\nu$ for $\nu \in \{1, \dots, p\}$ the variables which appear in $\lambda f_l + \mu g_l$ with a coefficient divisible by p are exactly those of colour ν. Consequently, if $I_\nu^l \geq I_\mu^l$ for all $0 \leq \mu \leq p$ it follows that $I_\nu^l = m_l - q_l$. Define $I_{\max}^l = m_l - q_l$. This notation can be generalised as follows.

Definition 4. For a set $\mathscr{K}$ of indices i of variables x_i at level l define $I_\nu(\mathscr{K})$ as the number of $i \in \mathscr{K}$ with x_i of colour ν, $I_{\max}(\mathscr{K}) = \max_{0 \leq \nu \leq p} I_\nu(\mathscr{K})$ and $q(\mathscr{K}) = |\mathscr{K}| - I_{\max}(\mathscr{K})$.

Note that if $\mathscr{K}$ is the set of all indices of variables at level l, then $|\mathscr{K}| = m_l$, $I_\nu(\mathscr{K}) = I_\nu^l$, $I_{\max}(\mathscr{K}) = I_{\max}^l$ and $q(\mathscr{K}) = q_l$.

From the definition of a non-singular solution it follows that whether a solution of (2.1.6) is non-singular depends exclusively on the variables at level 0. If a solution of (2.1.6) has variables at level 0 of at least two different colours set to a value which is not congruent to 0 modulo p, the corresponding matrix has rank 2 modulo p making it a non-singular solution. To use variables at different levels one can take sets of variables at one level and combine them in a way that they can be seen as a variable of a higher level. This method was introduced by Davenport and Lewis [14] and applied in combination with the notion of coloured variables by Brüdern and Godinho [8].

Definition 5. Let $\mathscr{K}$ be a set of indices j with x_j at level l. Let $h \in \mathbb{N}$ with $h > l$ and suppose that there are integers y_j with $p \nmid y_j$ such that

$$\sum_{j \in \mathscr{K}} a_j y_j^k \equiv \sum_{j \in \mathscr{K}} b_j y_j^k \equiv 0 \mod p^h. \tag{2.2.1}$$

Then $\mathscr{K}$ is called a *contraction from level l to level at least h*. If either $\sum_{j \in \mathscr{K}} a_j y_j^k$ or $\sum_{j \in \mathscr{K}} b_j y_j^k$ is not congruent to 0 modulo p^{h+1}, then $\mathscr{K}$ is called a *contraction from level l to level h*.

Recall for variables at level l that $\tilde{a}_j = p^{-l} a_j$ and $\tilde{b}_j = p^{-l} b_j$. Hence, a set $\mathscr{K}$ of variables at level l is a contraction to a variable at level at least $l + n$ if there are y_j not divisible by p such that

$$\sum_{j \in \mathscr{K}} \tilde{a}_j y_j^k \equiv \sum_{j \in \mathscr{K}} \tilde{b}_j y_j^k \equiv 0 \mod p^n.$$

If $\mathscr{K}$ is a contraction from level l to some level h, one can set $x_j = y_j X_0$ for all j in the contraction $\mathscr{K}$. Through this, one obtains a variable X_0 at level h. One says that the variable X_0 can be *traced back* to the variables x_j with $j \in \mathscr{K}$. Assume that there are other variables X_i at level h with $i \in \{1, \dots, n\}$, where each of the variables X_i is a variable at level h which either occurred in the pair f, g or is the result of a contraction. If the set of indices $\{0, 1, \dots, n\}$ of the variables $X_0, X_1, \dots, X_n$ is a contraction to a variable Y at a level at least $h + 1$, then one says that the variable Y can be traced back not only to the variables X_i for $i \in \{0, 1, \dots, n\}$ but also to all the variables that those variables can be traced back to. For example, Y can be traced back to all x_j with $j \in \mathscr{K}$.

Definition 6. A variable is called a *primary variable* if it can be traced back to two variables at level 0 of different colours.

If one can contract a primary variable at level at least γ, then by setting this contracted variable 1 and everything else zero, one obtains a non-singular solution of (2.1.6) and, therefore, a non-trivial p-adic solution.

In some cases the knowledge of the exact level and colour of a variable that was contracted gives quite an advantage. To gain control about this, the concept of coloured variables is not strong enough because it can only give the information whether a certain set of variables at level l is a contraction to a variable at level $l+1$ or at level at least $l+1$, but one does not know enough of the behaviour of the variables modulo p^{l+2}. Therefore, one cannot use it to extract information about the colour of the contracted variable. To gain this information, one can divide the set of variables of one colour into smaller sets which consider the level coefficient vectors $\binom{\tilde{a}_i}{\tilde{b}_i}$ not only modulo p but modulo p^2.

For that, view the vectors $\boldsymbol{e}_0 = \binom{1}{0}$ and $\boldsymbol{e}_\nu = \binom{\nu}{1}$ as vectors in $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^2$ and define the vectors $\boldsymbol{e}^0 = \binom{0}{p}$ and $\boldsymbol{e}^\nu = \binom{p}{0}$ for $\nu \in \{1, \dots, p-1\}$. This enables one to define sets similar to the sets $\mathscr{L}_\nu$ via

$$\mathscr{L}_{\nu\mu} := \left\{ c\left(\boldsymbol{e}_\nu + \mu \boldsymbol{e}^\nu\right) \mid c \in \left(\mathbb{Z}/p^2\mathbb{Z}\right)^* \right\}$$

for $0 \le \nu \le p$ and $0 \le \mu \le p-1$. Here again, a level coefficient vector $\binom{\tilde{a}_i}{\tilde{b}_i}$ lies modulo p^2 in exactly one of the disjoint sets $\mathscr{L}_{\nu\mu}$.

Definition 7. A variable x_i is said to be of *colour nuance* (ν, μ) if the level coefficient vector $\left(\tilde{a}_i, \tilde{b}_i\right)$ interpreted as a vector in $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^2$ lies in $\mathscr{L}_{\nu\mu}$. The parameter $I^l_{\nu\mu}$ of a pair f, g is the number of variables x_i at level l of colour nuance (ν, μ).

For all variables x_i of colour nuance (ν, μ) there is a unique integer $c_i \in \{1, 2, \dots, p^2\} \backslash p\mathbb{Z}$ for which $\binom{\tilde{a}_i}{\tilde{b}_i} \equiv c_i \left(\boldsymbol{e}_\nu + \mu \boldsymbol{e}^\nu\right) \bmod p^2$. The integer c_i is said to be the *corresponding integer* to x_i.

Lemmata 2 and 4 show that it suffices to find a non-singular solution for all p-normalised pairs in order to prove that for any rational coefficients a_j, b_j the equations (1.0.1) have a non-trivial solution in $\mathbb{Q}_p$. Due to Lemma 3 one already has some information about the number of variables at certain levels and the distribution of these variables in the different colours of p-normalised forms f, g. One can further exploit that every p-equivalence class contains more than just one p-normalised pair. The next lemma shows further properties that are fulfilled by at least one p-normalised pair in each p-equivalence class for which $\vartheta(f, g) \neq 0$ holds.

Lemma 5. *Each pair of diagonal forms* (2.1.1)*, with rational coefficients and* $\vartheta \neq 0$*, is* p*-equivalent to a* p*-normalised pair* f, g *possessing the following properties:*

(i) g_0 *contains exactly* q_0 *variables with coefficients not divisible by* p*.*

(ii) One of f_1, g_1 *contains exactly* q_1 *variables with coefficients not divisible by* p*.*

(iii) g_0 *has the form*

$$g_0 = p^2 \sum_{i=1}^{I^0_{00}} \alpha_i x_i^k + p \sum_{i=I^0_{00}+1}^{I^0_0} \beta_i x_i^k + \sum_{I^0_0+1}^{m_0} \gamma_i x_i^k,$$

where $\beta_{I_{00}^0+1}, \dots, \beta_{I_0^0}, \gamma_{I_0^0+1}, \dots, \gamma_{m_0}$ *are not divisible by* p*, and*

$$m_0 + m_1 - I_0^1 - \frac{s}{k} \geq I_{00}^0 \geq \frac{m_0 - q_0}{p}.$$

Furthermore, $I_{00}^0 \geq I_{0\mu}^0$ *for all* $0 \leq \mu \leq p-1$.

Proof. See [14, Lemma 10]. □

It follows from the first property that $I_{\max}^0 = I_0^0 = m_0 - q_0$. The second property shows that either $I_0^1 = m_1 - q_1$ or $I_p^1 = m_1 - q_1$ and, therefore, either the colour 0 or the colour p has the most variables at level 1. Note that it follows from the third property that

$$I_0^0 + q_0 + m_1 - I_0^1 - \frac{s}{k} \geq I_{00}^0 \geq \frac{I_0^0}{p}$$

and, thus, that

$$I_0^0 - I_{00}^0 \geq \frac{s}{k} - q_0 - \left(m_1 - I_0^1\right). \tag{2.2.2}$$

As every p-normalised pair is p-equivalent to a p-normalised pair possessing the properties of the previous lemma, it suffices to prove the existence of a non-singular solutions for p-normalised pairs with these properties.

By using only the variables at level 0 it was proved by Brüdern and Godinho [8, Section 4] that a pair f, g for which q_0 is large has a non-singular solution as displayed in the following.

They said that a colour ν is *zero-representing* if there is a subset $\mathscr{K}$ of variables at level 0 of colour ν for some $0 \leq \nu \leq p$, which is a contraction to a variable at level at least γ. The following Lemma is an immediate result from this definition.

Lemma 6. *If a pair* f, g *as in* (2.1.1) *has two colours that are zero-representing, then there exists a non-singular solution of* (2.1.6)*.*

Proof. See [8, Lemma 4.1]. □

Using a theorem of Olson [35], they then provided a lower bound of the amount of variables at level 0 of colour ν which are required in order to ensure that ν is zero-representing.

Lemma 7. *If* $I_\nu^0 \geq p^\gamma + p^{\gamma-1} - 1$*, then the colour* ν *is zero-representing.*

Proof. See [8, Lemma 4.2]. □

Using these two lemmata and the theorem of Olson [35] again, they concluded the following statement.

Lemma 8. *If a pair* f, g *as in* (2.1.1) *has* $q_0 \geq 2p^\gamma - 1$*, then there exists a non-singular solution of* (2.1.6)*.*

Proof. See [8, Lemma 4.4] □

Therefore, it suffices to focus on p-normalised forms f, g that fulfil the properties of Lemma 5 and have $q_0 \leq 2p^\gamma - 2$.

2.3 Combinatorial Results

This section contains a collection of lemmata with combinatorial results on congruences modulo p and p^2 for primes p, which is later convenient for finding contraction in certain sets.

Lemma 9. *Let $n > \mathrm{ggT}\,(k, p-1)$ and $c_1, \ldots, c_n$ be any integers coprime to p. Then, the congruence*

$$c_1 x_1^k + \cdots + c_n x_n^k \equiv 0 \mod p$$

has a solution with $x_1 \not\equiv 0 \bmod p$.

Proof. See [12, Lemma 1]. □

Lemma 10. *Let $\alpha_{ij} \in \mathbb{Z}$ for $1 \le i \le n$ and $1 \le j \le s$ with $s \ge np - n + 1$. Then the equation*

$$\sum_{j=1}^{s} \varepsilon_j \begin{pmatrix} \alpha_{1j} \\ \vdots \\ \alpha_{nj} \end{pmatrix} \equiv 0 \mod p$$

has a solution with $\varepsilon_j \in \{0, 1\}$ for $1 \le j \le s$ and some $\varepsilon_j \ne 0$.

Proof. This is the special case $G = (\mathbb{Z}/p\mathbb{Z})^n$ of the theorem of Olson [35]. □

Lemma 11. *Let $s \ge 3p - 2$ and $a_j, b_j \in \mathbb{Z}$ for $1 \le j \le s$. Then there exists a non-empty subset $J \subset \{1, 2, \ldots, s\}$ with $|J| \le p$ and $\sum_{j \in J} a_j \equiv \sum_{j \in J} b_j \equiv 0 \bmod p$.*

Proof. See [36, Lemma 1.1]. □

Lemma 12. *Let $d_j \in \mathbb{Z} \backslash p\mathbb{Z}$ for $1 \le j \le 3p - 2$. Then there exists a non-empty subset $J \subset \{1, \cdots, 3p-2\}$ with $|J| \le p$,*

$$\sum_{j \in J} d_j \equiv 0 \mod p \qquad \text{and} \qquad \sum_{j \in J} d_j \not\equiv 0 \mod p^2.$$

Proof. See [21, Lemma 3.7]. □

Lemma 13. *Let $d_j \in \mathbb{Z} \backslash 5\mathbb{Z}$ for $1 \le j \le 9$. Then there exists a non-empty subset $J \subset \{1, \cdots, 9\}$ with $|J| \le 5$,*

$$\sum_{j \in J} d_j \equiv 0 \mod 5 \qquad \text{and} \qquad \sum_{j \in J} d_j \not\equiv 0 \mod 25.$$

Proof. See [20, Proposition 3.1]. □

2.4 Strategy

This section contains a general description of the remainder of the proof, for which further notation is introduced. Assume for the remainder of this chapter that $\tau \ge 1$ is an integer, $p \ge 5$ a prime and $k = p^\tau (p-1)$. This is not be repeated in the following but nonetheless assumed in all following lemmata of this chapter.

Definition 8. A p-normalised pair of diagonal forms f, g as in (2.1.1) is called a *proper p-normalised pair* if $s \geq 2k^2 + 1$, $q_0 \leq 2p^{\tau+1} - 2$ and it satisfies the properties of Lemma 5.

The restrictions on k, p and τ show that $\gamma = \tau + 1$. Therefore, it follows from Lemmata 2, 5 and 8 that it suffices to prove for every proper p-normalised pair f, g that the equations $f = g = 0$ have a non-trivial p-adic solution.

The bound $s \geq 2k^2 + 1$ and Lemma 3 show that a proper p-normalised pair has the lower bounds

$$\begin{aligned} m_0 + \cdots + m_j &\geq (2j+2)\, p^{\tau+1} - (2j+2)\, p^{\tau} + 1, \\ m_0 + \cdots + m_{j-1} + q_j &\geq (2j+1)\, p^{\tau+1} - (2j+1)\, p^{\tau} + 1 \end{aligned}$$

for $j \in \{0, \ldots, k-1\}$ and furthermore, Lemma 5 provides

$$I_0^0 - I_{00}^0 \geq 2p^{\tau+1} - 2p^{\tau} - q_0 - \left(m_1 - I_0^1\right). \tag{2.4.1}$$

To find a non-trivial p-adic solution for a proper p-normalised pair, it suffices, due to Lemma 4, to show that a non-singular solution exists. Using contractions as described in Section 2.2, this can be done by showing that one can construct a primary variable at level $\tau + 1$.

In the following there are two different strategies to construct a primary variable at level at least $\tau + 1$. For the first, one contracts the variables at level 0 to primary variables at level at least 1. Using contractions recursively, one obtains primary variables at higher levels, until one eventually reaches at least level $\tau + 1$.

The second strategy is used if $I_0^0 \geq p^{\tau+1} + p^{\tau} - 1$. By Lemma 7 with $\gamma = \tau + 1$, it follows that the colour 0 is zero-representing. In this case it suffices to have a contraction to a variable at level at least $\tau + 1$, which can be traced back to at least one variable at level 0 of a different colour than 0. If such a variable can also be traced back to a variable at level 0 of colour 0, the variable is already primary. Else, there is a contraction to another variable at level at least $\tau + 1$, using only the variables at level 0 of colour 0. Setting both of these variables 1 and everything else zero proves that there is a non-singular solution of $f = g = 0$.

Definition 9. A variable which is either a variable at level 0 of a different colour than 0 or can be traced back to one is called *colourful*.

Thus, if $I_0^0 \geq p^{\tau+1} + p^{\tau} - 1$, the goal is to create a colourful variable at level at least $\tau + 1$.

The gain of this second strategy are the variables at level 0 of colour 0. To contract primary variables at level at least 1, one usually uses the variables at level 0. If the goal is only to contract colourful variables at level at least 1, it suffices to use the q_0 variables at level 0 which are colourful. Then, the variables at level 0 of colour 0 can be used to create variables at a higher level, to help contracting the colourful variables to colourful variables at an even higher level, until one eventually contracts them to a colourful variable at level at least $\tau + 1$. This works because one encounters one of the following two scenarios. Either the colourful variable at level at least $\tau + 1$ can be traced back to a variable at level 0 of colour 0. Then one has used one of those variables, which were created using the variables at level 0 of colour 0, some way along the way, and the colourful variable at level at least $\tau + 1$ is also primary. If on the other hand, the colourful variable at level at least $\tau + 1$ cannot be traced back to a variable at level 0 of colour 0, those helpful variables were not needed, to create a colourful variable at level at least $\tau + 1$. Hence, one can create a colourful variable at level at least $\tau + 1$, without

using any of the variables at level 0 of colour 0, which still enables one to create a variable at level at least $\tau+1$, using only those.

The process of creating a colourful or primary variable at level at least $\tau+1$ follows the same pattern. If one has a colourful or primary variable at level at least l, either this variable is already at level at least $l+1$, or one tries to find a contraction to a variable at level at least $l+1$, which contains the colourful or primary variable and thus ensures that the resulting variable at level $l+1$ is colourful or primary, as well. To find such a contraction, one needs to guarantee that there are other variables at the same level with certain properties. Thus, one distinguishes between the colourful and primary variables, for which one only needs to know a lower bound of their level, and the remaining variables, which are useful to contract colourful or primary variables to colourful and primary variables at a higher level. For them it is important to know the precise level they are at. This is considered by the following notation.

A primary variable at level at least l of colour nuance (ν,μ) is denoted by $P^l_{\nu\mu}$, whereas a colourful variable which otherwise has the same properties is denoted by $C^l_{\nu\mu}$. The notation $E^l_{\nu\mu}$ is used to describe a variable at the exact level l of colour nuance (ν,μ). Note that for $S\in\{C,P\}$ a variable of type $S^l_{\nu\mu}$ can either be of type $S^{l+1}_{\nu\mu}$ or of type $E^l_{\nu\mu}$, but not both. It is said throughout the proof that a set of variables contracts to a variable with certain properties, if one the following cases occur. Either one of the variables in the set is already a variable with the desired properties, or the set of indices of these variables contains a contraction to a variable with these properties. This helps to minimise the amount of cases in which one has to distinguish between an $S^l_{\nu\mu}$ variables being of type $S^{l+1}_{\nu\mu}$ or $E^l_{\nu\mu}$ for $S\in\{C,P\}$. Sometimes one only wants to establish the level and the colour of one variable. Then, this is denoted by P^l_ν, C^l_ν or E^l_ν. If even the colour is of no importance, such a variable is said to be of type P^l, C^l or E^l. In some cases, one has to denote that a variable of type E^l is not of colour ν, or that a variable of type E^l_ν is not of colour nuance (ν,μ). This is denoted by the bar over the related index in $E^l_{\bar\nu}$ and $E^l_{\nu\bar\mu}$, respectively.

It turns out that the number of C^1 and P^1 variables one can contract the E^0 variables to is at least partly dependent on the parameter q_0. Therefore, it is useful to define a further parameter $r=r(f,g)$ for a pair f,g which restricts the area for q_0 to

$$p^{\tau+1}+rp^\tau\le q_0\le p^{\tau+1}+(r+1)p^\tau-1. \tag{2.4.2}$$

For a proper p-normalised pair f,g it follows that $r=r(f,g)\in\{-1,0,1,\dots,p-1\}$ due to $p^{\tau+1}-p^\tau+1\le q_0\le 2p^{\tau+1}-2$.

2.5 Contraction Related Auxiliaries

This section is a compilation of settings in which sets of variables contract to variables at a higher level.

2.5.1 Contracting One Specific Variable

The lemmata in this subsection describe situations in which one contracts sets of variables to one variable with specific properties.

Lemma 14. *Let $\mathscr{K}$ be a set of indices of E^l variables. If $|\mathscr{K}|\ge 2p-1$ and $q(\mathscr{K})\ge p$, then $\mathscr{K}$ contains a contraction J to a variable at level at least $l+1$, such that J contains variables*

of at least two different colours.

Proof. This is a restatement of [14, Lemma 3]. □

Lemma 15. *Let $S \in \{C, P\}$. A set of $2p-1$ variables of type S^l contracts to an S^{l+1} variable.*

Proof. Either one of the S^l variables is already a variable of type S^{l+1} or Lemma 10 can be used with $n = 2$ to show that the set of indices of the $2p-1$ variables of type S^l contains a contraction to a variable at level at least $l+1$ which can be traced back to at least one of the S^l variables. Therefore, it is an S^{l+1} variable. □

Lemma 16. *Let $S \in \{C, P\}$ and let there be $3p-2$ variables of type S^l. Then one can contract them to a variable of type S^{l+1}, using at most p of them.*

Proof. Either one of the S^l variables is already a variable of type S^{l+1} or, due to Lemma 11, one can contract the S^l variables to a variable at level at least $l+1$ using at most p of them. This variable can be traced back to at least one of the S^l variables, thus it is an S^{l+1} variable. □

Lemma 17. *Let there be $3p-2$ variables of type E^l_ν for $p \geq 5$ and $2p-1$ variables of type E^l_ν for $p = 5$. Then one can contract at most p of these variables to a variable of type E^{l+1}.*

Proof. For $p \geq 5$ see [21, Lemma 3.10] and for $p = 5$ see [20, Lemma 3.8]. □

Lemma 18. *Let there be $3p-2$ variables of type $E^l_{\nu\mu}$ for $p \geq 5$ or $2p-1$ variables for $p = 5$. Then one can contract at most p variables to a variable of type E^{l+1}_ν.*

Proof. Let $\mathscr{K}$ be the set of indices of these variables. Let c_i be the corresponding integer of the variable x_i. Due to Lemma 12 for $p \geq 5$ and Lemma 13 for $p = 5$, there is a non-empty subset $J \subset \mathscr{K}$ with $|J| \leq p$, such that $\sum_{j\in J} c_j \equiv 0 \bmod p$ while $\sum_{j\in J} c_j \not\equiv 0 \bmod p^2$ and it follows that

$$\sum_{j\in J} \begin{pmatrix} \tilde{a}_j \\ \tilde{b}_j \end{pmatrix} \equiv \sum_{j\in J} c_j \left(\boldsymbol{e}_\nu + \mu \boldsymbol{e}^\nu\right) \equiv \left(\boldsymbol{e}_\nu + \mu \boldsymbol{e}^\nu\right) \sum_{j\in J} c_j \not\equiv 0 \mod p^2,$$

while $\sum_{j\in J} c_j \equiv 0 \bmod p$. As $p \mid \boldsymbol{e}^\nu$, this leaves

$$\sum_{j\in J} \begin{pmatrix} \tilde{a}_j \\ \tilde{b}_j \end{pmatrix} \equiv \boldsymbol{e}_\nu \sum_{j\in J} c_j \equiv pc\boldsymbol{e}_\nu \mod p^2$$

for some c not congruent to 0 modulo p. Hence, by setting $x_i = 1$ for all $i \in J$, one can see that J is a contraction of at most p variables to a variable of type E^{l+1}_ν. □

Lemma 19. *Let there be $p-1$ variables of type $E^l_{\nu\mu_1}$ and one of type $E^l_{\nu\mu_2}$ with $\mu_1 \neq \mu_2$. Then one can contract them to an $E^{l+1}_{\bar{\nu}}$ variable.*

Proof. Define x^{-1} for an integer $x \in \mathbb{Z}\backslash p\mathbb{Z}$ as the element in $\{1, \ldots, p-1\}$ which solves $x \cdot x^{-1} \equiv 1 \bmod p$.

Let $\mathscr{K}$ be the set of indices of those p variables and c_i be the corresponding integer for $i \in \mathscr{K}$. Let x_{i_0} be the $E^l_{\nu\mu_2}$ variable. Due to Lemma 9 there is a solution of

$$\sum_{i\in\mathscr{K}} c_i y_i^k \equiv tp \mod p^2$$

for some $t \in \{1, \dots, p\}$ with $y_{i_0} \not\equiv 0 \bmod p$. Consequently, one has $y_{i_0}^k \equiv 1 \bmod p$ because $p-1 \mid k$ and it follows that

$$\sum_{i \in \mathscr{K}} \begin{pmatrix} \tilde{a}_i \\ \tilde{b}_i \end{pmatrix} y_i^k \equiv \sum_{i \in \mathscr{K} \setminus \{i_0\}} c_i \left(\boldsymbol{e}_\nu + \mu_1 \boldsymbol{e}^\nu \right) y_i^k + c_{i_0} \left(\boldsymbol{e}_\nu + \mu_2 \boldsymbol{e}^\nu \right) y_{i_0}^k \equiv tp\boldsymbol{e}_\nu + c_{i_0} \boldsymbol{e}^\nu \left(\mu_2 - \mu_1 \right) \mod p^2,$$

which is divisible by p because $\boldsymbol{e}^\nu$ is. For $\nu = 0$ one has

$$\begin{aligned} tp\boldsymbol{e}_\nu + c_{i_0} \boldsymbol{e}^\nu \left(\mu_2 - \mu_1 \right) &\equiv p \left(t \begin{pmatrix} 1 \\ 0 \end{pmatrix} + c_{i_0} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \left(\mu_2 - \mu_1 \right) \right) \\ &\equiv p \left(c_{i_0} \left(\mu_2 - \mu_1 \right) \begin{pmatrix} t c_{i_0}^{-1} \left(\mu_2 - \mu_1 \right)^{-1} \\ 1 \end{pmatrix} \right) \mod p^2 \end{aligned}$$

because p divides neither c_{i_0} nor $\mu_2 - \mu_1$. It follows that the resulting variable lies at level $l+1$ and is of colour $\nu' \neq 0$ with $\nu' \equiv t c_{i_0}^{-1} \left(\mu_2 - \mu_1 \right)^{-1} \bmod p$. For $\nu \neq 0$ one gets

$$tp\boldsymbol{e}_\nu + c_{i_0} \boldsymbol{e}^\nu \left(\mu_2 - \mu_1 \right) \equiv p \left(t \begin{pmatrix} \nu \\ 1 \end{pmatrix} + c_{i_0} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \left(\mu_2 - \mu_1 \right) \right) \mod p^2$$

which is for $t \equiv 0 \bmod p$ congruent to

$$p \left(c_{i_0} \left(\mu_2 - \mu_1 \right) \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right)$$

and else congruent to

$$p \left(t \begin{pmatrix} \nu + t^{-1} c_{i_0} \left(\mu_2 - \mu_1 \right) \\ 1 \end{pmatrix} \right).$$

Again because p divides neither c_{i_0} nor $\mu_2 - \mu_1$, one obtains a variable at level $l+1$, which is for $t \equiv 0 \bmod p$ of colour 0 and for $t \not\equiv 0 \bmod p$ of colour ν' for $\nu' \equiv \nu + t^{-1} c_{i_0} \left(\mu_2 - \mu_1 \right) \bmod p$ with $\nu' \neq \nu$. □

Lemma 20. *Let $S \in \{C, P\}$ and $0 \leq m \leq p-1$. Let there be $p-m-1$ variables of type E_ν^l and $m+1$ of type S_ν^l. Then they contract to a variable of type S^{l+1}.*

Proof. Either one of the S_ν^l variables is already a S_ν^{l+1} variable, or one can assume that they are all of type E_ν^l as well. The cases $l > 0$ can be reduced to the case $l = 0$ by working with the level coefficient vector $\left(\begin{smallmatrix} \tilde{a}_i \\ \tilde{b}_i \end{smallmatrix}\right)$ instead of the coefficient vector $\left(\begin{smallmatrix} a_i \\ b_i \end{smallmatrix}\right)$. See [20, Lemma 3.7] for the case $l = 0$. □

Lemma 21. *Let $\mathscr{H}$ be a set of indices of variables of type E_ν^l with $|\mathscr{H}| \geq 4p-3$ and either for all $i \in \mathscr{H}$ the corresponding integer c_i is congruent to an element in the set $\left\{1, 2, \dots, \frac{p-1}{2}\right\}$ modulo p or all c_i are congruent to elements in the set $\left\{\frac{p+1}{2}, \dots, p-1\right\}$. Then $\mathscr{H}$ contains a contraction $\mathscr{K}$ to a variable of type E_ν^{l+1}, with $|\mathscr{K}| \leq 2p-2$.*

Proof. For all $i \in \mathscr{H}$, let (ν, μ_i) be the colour nuance of the variable x_i and let $d_i \in \{1, 2, \dots, p-1\}$ and $f_i \in \{0, 1, \dots, p-1\}$ be such that as $c_i = d_i + p f_i$.

For the proof one can assume that $|\mathscr{H}| = 4p-3$. If this is not the case, one can take a subset of $\mathscr{H}$ to obtain the desired result. The first part proves the weaker claim that $\mathscr{H}$ contains a

subset $\mathscr{K}$ containing at most $2p$ variables such that

$$\sum_{i\in J}\begin{pmatrix} d_i \\ d_i\mu_i \end{pmatrix} \equiv 0 \mod p \quad \text{and} \quad \sum_{i\in J}\begin{pmatrix} \tilde{a}_i \\ \tilde{b}_i \end{pmatrix} \equiv dp\boldsymbol{e}_\nu \mod p^2,$$

for some $d \not\equiv 0 \bmod p$. By Lemma 10, the set $\mathscr{H}$ contains a non-empty subset J such that

$$\sum_{i\in J}\begin{pmatrix} d_i \\ d_i\mu_i \\ f_i \\ 1 \end{pmatrix} \equiv 0 \mod p. \tag{2.5.1}$$

This leads to

$$\begin{aligned}\sum_{i\in J}\begin{pmatrix} \tilde{a}_i \\ \tilde{b}_i \end{pmatrix} &\equiv \sum_{i\in J} c_i\left(\boldsymbol{e}_\nu + \mu_i\boldsymbol{e}^\nu\right) \equiv \sum_{i\in J}\left(d_i + f_ip\right)\left(\boldsymbol{e}_\nu + \mu_i\boldsymbol{e}^\nu\right)\\ &\equiv \sum_{i\in J} d_i\boldsymbol{e}_\nu + \sum_{i\in J} d_i\mu_i\boldsymbol{e}^\nu + \sum_{i\in J} f_ip\boldsymbol{e}_\nu + \sum_{i\in J} f_ip\mu_i\boldsymbol{e}^\nu\\ &\equiv \boldsymbol{e}_\nu\sum_{i\in J} d_i \mod p^2,\end{aligned}$$

where the last equivalence holds due to $p \mid \boldsymbol{e}^\nu$ and the second and third entry in (2.5.1). The first entry shows that this is congruent to 0 modulo p. As J is a non-empty subset of $\mathscr{H}$, it follows from the fourth entry that $|J| \in \{p, 2p, 3p\}$. If $|J| = 3p$, take a subset $\tilde{J} \subset J$ containing $3p-2$ elements. By Lemma 10 with $n = 3$, there is a subset $\hat{J} \subseteq \tilde{J}$ with

$$\sum_{i\in \hat{J}}\begin{pmatrix} d_i \\ d_i\mu_i \\ f_i \end{pmatrix} \equiv 0 \mod p,$$

and, hence,

$$\sum_{i\in \hat{J}}\begin{pmatrix} \tilde{a}_i \\ \tilde{b}_i \end{pmatrix} \equiv \boldsymbol{e}_\nu\sum_{i\in \hat{J}} d_i \mod p^2,$$

as before, which again is congruent to 0 modulo p. As $J = \hat{J} \cup \left(J\backslash\hat{J}\right)$, it follows that

$$\sum_{i\in J\backslash\hat{J}}\begin{pmatrix} d_i \\ d_i\mu_i \\ f_i \end{pmatrix} \equiv 0 \mod p,$$

and, therefore,

$$\sum_{i\in J\backslash\hat{J}}\begin{pmatrix} \tilde{a}_i \\ \tilde{b}_i \end{pmatrix} \equiv \boldsymbol{e}_\nu\sum_{i\in J\backslash\hat{J}} d_i \mod p^2,$$

which is congruent to 0 modulo p as well. Furthermore, both sets $\hat{J}$ and $J\backslash\hat{J}$ are non-empty, and the smallest of them has at most $\frac{3p}{2} \le 2p$ elements. It follows that in every case there is a

non-empty set $\mathscr{K} \subset \mathscr{H}$ containing at most $2p$ elements, such that

$$\sum_{i\in J}\begin{pmatrix}\tilde{a}_i\\ \tilde{b}_i\end{pmatrix} \equiv \boldsymbol{e}_\nu \sum_{i\in J} d_i \mod p^2, \qquad \text{and} \qquad \sum_{i\in J}\begin{pmatrix} d_i\\ d_i\mu_i\end{pmatrix} \equiv 0 \mod p.$$

Assume now for such a set $\mathscr{K}$ that all corresponding integers c_i are congruent to elements in the set $\left\{1,2,\ldots,\frac{p-1}{2}\right\}$ modulo p. It follows that d_i lies in the same set for all $i \in \mathscr{K}$. Hence, it can be deduced from

$$1 \leq \sum_{i\in\mathscr{K}} d_i \leq \sum_{i\in\mathscr{K}} \frac{p-1}{2} \leq p\,(p-1)\,,$$

that $\sum_{i\in\mathscr{K}} d_i \not\equiv 0 \bmod p^2$ and, therefore,

$$\sum_{i\in\mathscr{K}}\begin{pmatrix}\tilde{a}_i\\ \tilde{b}_i\end{pmatrix} \equiv dp\boldsymbol{e}_\nu \mod p^2$$

for some $d \not\equiv 0 \bmod p$. This proves the weaker claim if all c_i are modulo p congruent to an element in the set $\{1,\ldots,\frac{p-1}{2}\}$. Now let all c_i be congruent to elements in the set $\left\{\frac{p+1}{2},\ldots,p-1\right\}$. It follows that

$$\begin{pmatrix}-\tilde{a}_i\\ -\tilde{b}_i\end{pmatrix} \equiv \left(p^2-c_i\right)\left(\boldsymbol{e}_\nu+\mu_i\boldsymbol{e}^\nu\right) \equiv \left(p-d_i+p\,(p-f_i-1)\right)\left(\boldsymbol{e}_\nu+\mu_i\boldsymbol{e}^\nu\right) \mod p^2$$

and that the corresponding integers $p-d_i+p\,(p-f_i-1)$ lie modulo p in $\left\{1,2,\ldots,\frac{p-1}{2}\right\}$, again. Using the obtained results, there is a subset $\mathscr{K} \subset \mathscr{H}$ with $|\mathscr{K}| \leq 2p$ and

$$\sum_{j\in\mathscr{K}}\begin{pmatrix}-\tilde{a}_j\\ -\tilde{b}_j\end{pmatrix} \equiv dp\boldsymbol{e}_\nu \mod p^2$$

for some $d \not\equiv 0 \bmod p$ and, as $\binom{\tilde{a}_i}{\tilde{b}_i}$ lies in the same set $\mathscr{L}_{\nu\mu}$ as $\binom{-\tilde{a}_i}{-\tilde{b}_i}$, one further has

$$\sum_{j\in\mathscr{K}}\begin{pmatrix}p-d_j\\ (p-d_j)\,\mu_j\end{pmatrix} \equiv 0 \mod p.$$

It follows that

$$\sum_{j\in\mathscr{K}}\begin{pmatrix}\tilde{a}_j\\ \tilde{b}_j\end{pmatrix} = -\sum_{j\in\mathscr{K}}\begin{pmatrix}-\tilde{a}_j\\ -\tilde{b}_j\end{pmatrix} \equiv -dp\boldsymbol{e}_\nu \mod p^2$$

for some $d \not\equiv 0 \bmod p$ and it further holds that

$$\sum_{j\in\mathscr{K}}\begin{pmatrix}d_j\\ d_j\mu_j\end{pmatrix} \equiv 0 \mod p.$$

This completes the proof for the weaker claim. Now let $\mathscr{K} \subset \mathscr{H}$ be a subset with $|\mathscr{K}| \leq 2p$,

$$\sum_{i\in\mathscr{K}}\begin{pmatrix}d_i\\ d_i\mu_i\end{pmatrix} \equiv 0 \mod p \quad \text{and} \quad \sum_{i\in\mathscr{K}}\begin{pmatrix}\tilde{a}_i\\ \tilde{b}_i\end{pmatrix} \equiv pd\boldsymbol{e}_\nu \mod p^2$$

for some $d \not\equiv 0 \bmod p$. Assuming that $|\mathscr{K}| \geq 2p-1$, there is, according to Lemma 10 with $n = 2$, a subset $\tilde{\mathscr{K}} \subset \mathscr{K}$ with $|\tilde{\mathscr{K}}| \leq 2p-1$ and

$$\sum_{i \in \tilde{\mathscr{K}}} \binom{d_i}{d_i \mu_i} \equiv 0 \mod p.$$

It follows that

$$\sum_{i \in \tilde{\mathscr{K}}} \binom{\tilde{a}_i}{\tilde{b}_i} \equiv \boldsymbol{e}_\nu \sum_{i \in \tilde{\mathscr{K}}} d_i + p \boldsymbol{e}_\nu \sum_{i \in \tilde{\mathscr{K}}} f_i \mod p^2,$$

which is congruent to 0 modulo p, but not necessarily incongruent to 0 modulo p^2. As

$$\sum_{i \in \mathscr{K} \setminus \tilde{\mathscr{K}}} \binom{d_i}{d_i \mu_i} \equiv 0 \mod p$$

holds as well, one can deduce that

$$\sum_{i \in \mathscr{K} \setminus \tilde{\mathscr{K}}} \binom{\tilde{a}_i}{\tilde{b}_i} \equiv \boldsymbol{e}_\nu \sum_{i \in \mathscr{K} \setminus \tilde{\mathscr{K}}} d_i + p \boldsymbol{e}_\nu \sum_{i \in \mathscr{K} \setminus \tilde{\mathscr{K}}} f_i \mod p^2,$$

which is again congruent to 0 modulo p. For at least one of those sets, either $\tilde{\mathscr{K}}$ or $\mathscr{K} \setminus \tilde{\mathscr{K}}$, the sum is not congruent to 0 modulo p^2 as the sum over all $i \in \mathscr{K}$ is not, and, therefore, it is impossible for both subsums to be congruent to 0 modulo p^2. The set for which this sum is incongruent to 0 modulo p^2 is a contraction to a variable of type E_ν^{l+1}.

Both subsets are non-empty and, hence, as all d_i are incongruent to 0 modulo p, they contain at least 2 elements. Thus, each one has a most $2p-2$ elements, which proves the claim. □

Lemma 22. *Let $S \in \{C, P\}$ and $0 \leq m \leq p-1$. Let there be $p+m$ variables of type S^l and further $p-m-1$ variables of type E_ν^l. Then one can contract them to an S^{l+1} variable.*

Proof. If one of the S^l variables is already an S^{l+1} variable, the claim is fulfilled. Thus, one can assume that the S^l variables are E^l variables as well. If there are p variables of the same colour μ, then at least one of them is an S^l variables, because there are at most $p-1$ variables which are not. Hence, Lemma 20 shows that one can contract them to an S^{l+1} variable.

Else, there are at most $p-1$ variables of the same colour. Let $\mathscr{K}$ be the set of indices of all $2p-1$ variables. Then, one has $I_{\max}(\mathscr{K}) \leq p-1$, and thus, $q(\mathscr{K}) \geq p$. By Lemma 14, the set $\mathscr{K}$ contains a contraction to to a variable at level at least $l+1$, using at least two different colours. One can trace that variable back to at least one of the S^l variables, because the variables which are not of type S^l are all of the same colour, which proves the claim. □

Lemma 23. *Let $S \in \{C, P\}$ and $0 \leq m \leq p-1$. Let there be $p-1$ variables of type E_ν^l, $p-m-1$ variables of type $E_{\bar{\nu}}^l$ and $m+1$ variables of type S^l. Then one can contract them to an S^{l+1} variable.*

Proof. If one of the variable of type S^l is already an S^{l+1} variable, the claim is fulfilled, thus one can assume that these variables are of type E^l as well. Furthermore, one can assume that none of the S^l variables is of type S_ν^l, because else, Lemma 20 can be use to contract the $p-1$ variables of type E_ν^l together with the S_ν^l variable to an S^{l+1} variable.

Therefore, one can assume that one has $p-1$ variables of type E_ν^l and p variables of type $E_{\tilde{\nu}}^l$ from which at least one is an S^l variable. For convenience name the E_ν^l variables $x_1,\dots,x_{p-1}$ and the $E_{\tilde{\nu}}^l$ variables $x_p,\dots,x_{2p-1}$, where x_{2p-1} is an S^l variable. Furthermore, let c_i be the corresponding integer of x_i for $1 \le i \le 2p-1$ and $\nu_i \neq \nu$ the colour of the variables x_i for $p \le i \le 2p-1$. These $2p-1$ variables contract to an S^{l+1} variable if there is a solution of

$$\sum_{i=1}^{p-1} c_i \boldsymbol{e}_\nu x_i^k + \sum_{i=p}^{2p-1} c_i \boldsymbol{e}_{\nu_i} x_i^k \equiv 0 \mod p,$$

with $x_{2p-1} \not\equiv 0 \bmod p$. The existence of such a solution follows from the proof of Theorem 2 by Olson and Mann [32], but not from the statement of the theorem, from which one can only conclude the existence of a solution, but not that one has one with $x_{2p-1} \not\equiv 0 \bmod p$. Thus, for the convenience of the reader, the following contains a proof that such a solution exists. In essence the proof uses the same methods as the proof by Olson and Mann, but is tailored for this exact case.

By applying the linear transformation induced by

$$\begin{pmatrix} 1 & 0 \\ 1 & -\nu \end{pmatrix}$$

if $\nu \neq 0$, one can transform the case $\nu \neq 0$ to the case $\nu = 0$, because

$$\begin{pmatrix} 1 & 0 \\ 1 & -\nu \end{pmatrix} \boldsymbol{e}_\nu = \nu \boldsymbol{e}_0 \qquad \text{and} \qquad \begin{pmatrix} 1 & 0 \\ 1 & -\nu \end{pmatrix} \boldsymbol{e}_{\nu_i} \in \mathscr{L}_{\tilde{\nu}}$$

for some $\tilde{\nu} \neq \nu$. All that remains is to solve a system of the kind

$$\sum_{i=1}^{p-1} \begin{pmatrix} \alpha_i \\ 0 \end{pmatrix} x_i^k + \sum_{i=p}^{2p-1} \begin{pmatrix} \beta_i \\ \gamma_i \end{pmatrix} x_i^k \equiv 0 \mod p \tag{2.5.2}$$

where $p \nmid \alpha_i$ for $1 \le i \le p-1$ and $p \nmid \gamma_i$ for $p \le i \le 2p-1$ such that $p \nmid x_{2p-1}$. By Lemma 9, there is a solution y_i with $p \le i \le 2p-1$ of the equation

$$\sum_{i=p}^{2p-1} \gamma_i y_i^k \equiv 0 \mod p$$

with $y_{2p-1} \not\equiv 0 \bmod p$. This reduces the system (2.5.2) by setting $x_i = y_i$ for $p \le i \le 2p-1$ to

$$\sum_{i=1}^{p-1} \alpha_i x_i^k + C \equiv 0 \mod p \tag{2.5.3}$$

for $C = \sum_{i=p}^{2p-1} \beta_i y_i^k$. Now consider an additional variable y_0. If $p \nmid y_0$ then $y_0^k \equiv 1 \bmod p$, hence, applying Lemma 9 again, this time to the system

$$\sum_{i=1}^{p-1} \alpha_i x_i^k + C y_0^k \equiv 0 \mod p$$

provides a solution y_i with $p \nmid y_0$. It follows that $x_i = y_i$ for $1 \le i \le p-1$ is also a solution for

(2.5.3) and, therefore, one has a solution of (2.5.2) given by $x_i = y_i$ with $1 \le i \le 2p-1$ with $p \nmid x_{2p-1}$. This completes the proof. □

2.5.2 Contracting Several Variables

The lemmata in this section show how to contract a set of variables at level at least l to another set of variables at level at least $l+1$.

Lemma 24. *Let $\mathscr{H} \subset \{1, \dots, m_0\}$ be a subset of indices of variables at level 0. Then $\mathscr{H}$ contains at least*

$$\min\left(\left\lfloor \frac{|\mathscr{H}|}{2p-1} \right\rfloor, \left\lfloor \frac{q(\mathscr{H})}{p} \right\rfloor\right)$$

pairwise disjoint contractions to variables of type P^1.

Proof. This is the special case $\delta = \gcd(k, p-1) = p-1$ of a result from Lemmata 1 and 3 of [14] which is proved in the second paragraph of Section 6 of that paper. □

Lemma 25. *Let $S \in \{C, P\}$ and let there be x variables of type S^l. They contract to $\left\lceil \frac{x+3}{p} \right\rceil - 3$ variables of type S^{l+1}, where each contraction contains at most p variables, leaving at least $\min\{2p-2, x\}$ variables of type S^l unused.*

Proof. For $x \le 3p-3$ the statement is trivial. Therefore, let $x \ge 3p-2$. Assume first that all x variables are also of type E^l. Then there is a contraction of at most p variables to an S^{l+1} variable due to Lemma 16. Hence, after doing this $\left\lceil \frac{x+3}{p} \right\rceil - 4$ times, there are still at least

$$x - \left(\left\lceil \frac{x+3}{p} \right\rceil - 4\right)p \ge x - (x + 3 + p - 1 - 4p) = 3p - 2$$

unused S^l variables. Hence, one can apply Lemma 16 once more, to obtain $\left\lceil \frac{x+3}{p} \right\rceil - 3$ contractions, leaving at least $2p-2$ variables unused. Thus, in this case, the claim holds.

Now assume that of the x variables of type S^l there are y variables already of type S^{l+1} while the remaining $x-y$ variables are of type E^l. One has

$$y \ge \left\lceil \frac{x+3}{p} \right\rceil - 3 + 2p - 2 - (x - y)$$

because of $x \ge 3p-2$. If $x - y \le 2p-2$, one can divide the y variables of type S^{l+1} in one set containing $\left\lceil \frac{x+3}{p} \right\rceil - 3$ and one set containing $2p - 2 - (x-y)$ of them. The variables in the second set together with the remaining $x-y$ variables of type S^l are at least $2p-2$ variables of type S^l, while the first set contains the $\left\lceil \frac{x+3}{p} \right\rceil - 3$ variables of type S^{l+1}. Thus, one can assume that $x - y \ge 2p-1$ and use the first part of this proof. The set of the $x-y$ variables of type E^l contains at least

$$\left\lceil \frac{x-y+3}{p} \right\rceil - 3$$

contractions to variables of type S^{l+1}, leaving at least $2p-2$ variables of type S^l unused. Together with the y variables of type S^{l+1} this gives at least

$$\left\lceil \frac{x-y+3}{p} \right\rceil - 3 + y = \left\lceil \frac{x-y+3}{p} + y \right\rceil - 3 = \left\lceil \frac{x+y\,(p-1)+3}{p} \right\rceil - 3 \geq \left\lceil \frac{x+3}{p} \right\rceil - 3$$

to variable of type S^{l+1}. □

Lemma 26. *Let there be x variables of type E_ν^l. They contract to $\left\lceil \frac{x}{2p-2} \right\rceil - 4$ variables of type E_ν^{l+1}, leaving at least $\min\{6p-9, x\}$ variables of type E_ν^l unused.*

Proof. For $x < 8p-7$ the statement is trivial. If $x \geq 8p-7$, one can divide the x variables in two sets. Those for which the corresponding integer c_i is congruent to one element in $\{1, \ldots, \frac{p-1}{2}\}$ modulo p, and the remaining variables. As long as there are at least $8p-7$ variables left, at least one of these sets contains at least $4p-3$ variables, which indicates that one can contract at most $2p-2$ of them to a variable of type E_ν^{l+1} due to Lemma 21. Doing this $\left\lceil \frac{x}{2p-2} \right\rceil - 5$ times leaves at least

$$x - (2p-2)\left(\left\lceil \frac{x}{2p-2} \right\rceil - 5\right) \geq x - x - 2p + 3 + 10p - 10 = 8p - 7$$

unused variables, hence, there is another contraction, leaving at least $6p-9$ variables unused. □

Lemma 27. *A set of $x \geq 3p^2 - 3p + 1$ variables of type E_ν^l contracts to $\left\lceil \frac{x}{p} \right\rceil - 2p + \frac{p-3}{2}$ variables of type E_ν^{l+1} for $p \geq 5$. A set of $x \geq 2p^2 - 2p + 1$ variables of type E_ν^l contracts to $\left\lceil \frac{x}{p} \right\rceil - 2p + 3$ variables of type E_ν^{l+1} for $p = 5$. In both cases, this leaves at least $6p-9$ of the E_ν^l variables unused.*

Proof. A set of at least $(3p-3)\,p+1$ variables of type E_ν^l contains at least $3p-2$ variables which are of the same colour nuance. By Lemma 18, one can contract at most p variables of them to a variable of type E_ν^{l+1}. Repeating this as often as possible provides $\left\lceil \frac{x}{p} \right\rceil - 3p + 3$ variables of type E_ν^{l+1} and leaves at least

$$x - p\left(\left\lceil \frac{x}{p} \right\rceil - 3p + 3\right) \geq x - \left(x + p - 1 - 3p^2 + 3p\right) = 3p^2 - 4p + 1$$

unused E_ν^l variables. For $p = 5$ this can be done as long as there are at least $(2p-2)\,p+1$ variables left. Therefore, one can do it $\left\lceil \frac{x}{p} \right\rceil - 2p + 2$ times, leaving at least

$$x - p\left(\left\lceil \frac{x}{p} \right\rceil - 2p + 2\right) \geq x - \left(x + p - 1 - 2p^2 + 2p\right) = 2p^2 - 3p + 1$$

unused variables. Using Lemma 26 provides another $p + \frac{p-1}{2} - 4$ variables of type E_ν^{l+1} for $p \geq 5$ and one for $p = 5$, while leaving at least $6p-9$ unused variables. All in all, one obtains

$$\left\lceil \frac{x}{p} \right\rceil - 3p + 3 + p + \frac{p-1}{2} - 4 = \left\lceil \frac{x}{p} \right\rceil - 2p + \frac{p-3}{2}$$

variables of type E_ν^{l+1} for $p \geq 5$ and

$$\left\lceil \frac{x}{p} \right\rceil - 2p + 2 + 1 = \left\lceil \frac{x}{p} \right\rceil - 2p + 3$$

for $p = 5$. □

Lemma 28. *Let $S \in \{C, P\}$ and x, y and z be non-negative integers with $y + z \geq (2 - m)\, p - 2$ for some $m \in \{0, 1, 2\}$ and $x - m \geq 0$. Let there be $(p-1)\, y$ variables of type E_ν^l, $(p-1)\, y$ variables of type $E_{\tilde{\nu}}^l$ and $px + y + z$ variables of type S^l. Then one can contract them to $x + y - m$ variables of type S^{l+1} without using $z + mp$ of the variables of type S^l.*

Proof. Using Lemma 16 to contract p of the variables of type S^l to an S^{l+1} variable can be done $x - m$ times. This leaves $y + z + mp \geq 2p - 2$ variables of type S^l. Then one can construct y sets, each consisting of one S^l variable, $p - 1$ variables of type E_ν^l and $p - 1$ variables of type $E_{\tilde{\nu}}^l$. By Lemma 23, each of this sets contains a contraction to an S^{l+1} variable, giving a total of $x + y - m$ variables of type S^{l+1} as claimed, without using $z + mp$ variables of type S^l. □

Lemma 29. *Let $S \in \{C, P\}$ and x be a non-negative integer. Let $\mathscr{K}$ be a set of E^l variables with $|\mathscr{K}| \geq (2p-2)\, x + p^2 - 3p + 1$ and $q(\mathscr{K}) \geq (p-1)\, x$ and let there be further x variables of type S^l. Then one can contract them to x variables of type S^{l+1}.*

Proof. The first part of the proof shows via induction on x that the set $\mathscr{K}$ contains x distinct sets S_i with $|S_i| = 2p - 2$ and $q(S_i) = p - 1$ for all $1 \leq i \leq x$.

For $x = 0$ the statement is true. It suffices to show for $x \geq 1$ that $\mathscr{K}$ contains a set $\mathscr{H}$ with $|\mathscr{H}| = 2p - 2$ and $q(\mathscr{H}) = p - 1$ such that $|\mathscr{K} \backslash \mathscr{H}| \geq (x-1)(2p-2) + p^2 - 3p + 1$ and $q(\mathscr{K} \backslash \mathscr{H}) \geq (x-1)(p-1)$. If such a set $\mathscr{H}$ exists, the induction hypothesis ensures that one can find further $x - 1$ distinct sets in $\mathscr{K} \backslash \mathscr{H}$.

Let $|\mathscr{K}| = x(2p-2) + p^2 - 3p + 1 + \alpha$ and $q(\mathscr{K}) = x(p-1) + \beta$ with $\alpha, \beta \in \mathbb{N}_0$. As $x \geq 1$ it follows that $q(\mathscr{K}) \geq p - 1$ and $|\mathscr{K}| \geq p^2 - p - 1 = (p+1)(p-2) + 1$, hence, $I_{\max}(\mathscr{K}) = I_\nu(\mathscr{K}) \geq p - 1$ for some $0 \leq \nu \leq p$. Thus, one can take $\mathscr{H}$ as a set containing $p - 1$ variables of type E_ν^l and $p - 1$ variables of type $E_{\tilde{\nu}}^l$ from which it follows that $|\mathscr{H}| = 2p - 2$, $q(\mathscr{H}) = p - 1$ and

$$|\mathscr{K} \backslash \mathscr{H}| = |\mathscr{K}| - 2p + 2 \geq (x-1)(2p-2) + p^2 - 3p + 1.$$

For $\beta \geq p - 1$ one has the trivial bound

$$q(\mathscr{K} \backslash \mathscr{H}) \geq q(\mathscr{K}) - 2(p-1) = (x-1)(p-1) + \beta - (p-1) \geq (x-1)(p-1),$$

whereas for $\beta \leq p - 2$ it follows that

$$\begin{aligned} I_{\max}(\mathscr{K}) = |\mathscr{K}| - q(\mathscr{K}) &= x(p-1) + \beta + \alpha + p^2 - 3p + 1 - 2\beta \\ &\geq q(\mathscr{K}) + p^2 - 5p + 5 \geq q(\mathscr{K}) \end{aligned}$$

and thus

$$q(\mathscr{K} \backslash \mathscr{H}) = q(\mathscr{K}) - (p-1) \geq (x-1)(p-1).$$

It follows that the set $\mathscr{K}$ contains x distinct sets S_i with $|S_i| = 2p - 2$ and $q(S_i) = p - 1$.

For each set S_i there is a ν_i such that $I_{\max}(S_i) = I_{\nu_i}(S_i) = p-1$. For $i \in \{1,\dots,x\}$ take the set S_i and one variable of type S^l, which gives $p-1$ variables of type $E^l_{\nu_i}$, $p-1$ variables of type $E^l_{\bar{\nu}_i}$ and one S^l variable. Such a set contains a contraction to an S^{l+1} variable due to Lemma 23. Thus, one obtains x variables of type S^{l+1}. □

Lemma 30. *Let $S \in \{C,P\}$ and x, y and z be non-negative integers with $y+z \geq (2-m)p-2$ for some $m \in \{0,1,2\}$ and $x-m \geq 0$. Let there be $(2p-2)y+p^2-3p+1$ variables of type E^l from which at least $(p-1)y$ variables are of type $E^l_{\bar{\nu}}$ for any $0 \leq \nu \leq p$. Furthermore, let there be $px+y+z$ variables of type S^l. Then one can contract them to $x+y-m$ variables of type S^{l+1} without using $z+mp$ of the variables of type S^l.*

Proof. Using Lemma 16 to contract p of the variables of type S^l to an S^{l+1} variable can be done $x-m$ times. This leaves $y+z+mp \geq 2p-2$ variables of type S^l. One can contract y of them together with the variables of type E^l to y variables of type S^{l+1} due to Lemma 29. This gives a total of $x+y-m$ variables of type S^{l+1} as claimed, without using $z+mp$ variables of type S^l. □

Lemma 31. *Let x be a non-negative integer. Let there be at least $px+p^2-3p+3$ variables of type E^l_ν from which at least x are of type $E^l_{\nu\mu}$ for some μ and at least x are of type $E^l_{\nu\bar{\mu}}$. Then one can contract px of them to x variables of type $E^{l+1}_{\bar{\nu}}$.*

Proof. Divide the E^l_ν variables in three sets. One contains x variables of type $E^l_{\nu\mu}$, the next contains x variables of type $E^l_{\nu\bar{\mu}}$ and the last contains the remaining variables.

The statement is trivial for $x=0$, thus one can assume that $x \geq 1$. Assume now that the last set contains $z \geq (p-2)p+1 = p^2-2p+1$ variables, and the first two both contain $y \geq 1$ variables. Then there is an η such that the last set contains at least $p-1$ variables of type $E^l_{\nu\eta}$ and one can choose one variable in one of the first two sets, which is of type $E^l_{\nu\bar{\eta}}$. These p variables contract to an $E^{l+1}_{\bar{\nu}}$ variable due to Lemma 19. Then, one can take one variable in the untouched set and put it in the last set, such that the first two sets both contain $y-1$ variables and the last one contains $z-p+2$ variables.

Starting with $z \geq (p-2)x+p^2-3p+3$ and $y=x$, after following this process $x-1$ times, one still has at least p^2-2p+1 variables in the last set left, while the other two each contain one variable. It follows that one can contract one more variable of type $E^{l+1}_{\bar{\nu}}$ as described above, giving a total of x variables of type $E^{l+1}_{\bar{\nu}}$. □

2.5.3 Inductive Contractions

This subsection uses induction to contract sets of variables at some level to variables more than one level higher.

Lemma 32. *Let $S \in \{C,P\}$ and $i,j \in \mathbb{N}_0$ with $i \leq j \leq \tau$ as well as $m \in \mathbb{Z}$ with $m \geq -1$. Let there be $p^{\tau-i+1}+mp^{\tau-i}-2$ variables of type S^i. Then one can contract them to $p^{\tau-j+1}+mp^{\tau-j}-2$ variables of type S^j and at least $2p-2$ variables of type S^l for all $l \in \{i,\dots,j-1\}$.*

Proof. For $i=j$ the statement is trivial, thus, the cases $i<j\leq\tau$ remain. Assume for an $l \in \{i,\dots,j-1\}$ that there are $p^{\tau-l+1}+mp^{\tau-l}-2$ variables of type S^l and $2p-2$ variables of type S^n for all $n \in \{i,\dots,l-1\}$. Lemma 25 shows that these variables can be contracted to

$$\left\lceil \frac{p^{\tau-l+1}+mp^{\tau-l}+1}{p} \right\rceil - 3 = p^{\tau-l}+mp^{\tau-l-1}-2$$

variables of type S^{l+1}. This leaves at least $2p-2$ variables of type S^l unused. The claim follows via induction. □

Lemma 33. *Let $S \in \{C, P\}$ and $i, j \in \mathbb{N}_0$ with $i \leq j \leq \tau$ as well as $m \in \mathbb{Z}$ with $m \geq -1$. Let there be $p^{\tau-i+1} + mp^{\tau-i}$ variables of type S^i and for all $l \in \{i, \dots, j-1\}$ let there be an ν_l and $2p-2$ variables of type $E^l_{\nu_l}$. Then one can contract them to $p^{\tau-j+1} + mp^{\tau-j}$ variables of type S^j.*

Proof. For $i = j$ the statement is trivial, thus, the cases $i < j \leq \tau$ remain. Assume for an $l \in \{i, \dots, j-1\}$ there are $p^{\tau-l+1} + mp^{\tau-l}$ variables of type S^l and $2p-2$ variables of type $E^l_{\nu_l}$. Lemma 25 shows that there exist

$$\left\lceil \frac{p^{\tau-l+1} + mp^{\tau-l} + 3}{p} \right\rceil - 3 = p^{\tau-l} + mp^{\tau-l-1} - 2$$

contractions to variables S^{l+1}, each of them containing at most p variables. Therefore, there are even $2p$ variables of type S^l remaining. Together with the $2p-2$ variables of type $E^l_{\nu_l}$, they can be contracted to another two S^{l+1} variables, using Lemma 22 twice. This gives a total of $p^{\tau-l} + mp^{\tau-l-1}$ variables of type S^{l+1}. The claim follows via induction. □

Lemma 34. *Let $m \leq p-1$ be an integer and let there be a $j \in \{0, 1, \dots, \tau-1\}$ such that there are*

$$2p^{\tau-j+1} + (4-2m)\,p^{\tau-j} - \frac{p-1}{2} \sum_{i=1}^{\tau-j-1} p^i + (2m-1)\,p^{\tau-j-1} + 3 \sum_{i=0}^{\tau-j-2} p^i - 2p - 2,$$

variables of type E^j_ν. Then one can contract them to $p-m-1$ variables of type E^τ_ν and $2p-2$ variables of type E^i_ν for all $i \in \{j, j+1, \dots, \tau-1\}$.

Proof. If $j \leq \tau-2$, assume that for some $l \in \{j, j+1 \dots, \tau-2\}$ one can contract the variables to $2p^{\tau-l+1} + (4-2m)\,p^{\tau-l} - \frac{p-1}{2} \sum_{i=1}^{\tau-l-1} p^i + (2m-1)\,p^{\tau-l-1} + 3\sum_{i=0}^{\tau-l-2} p^i - 2p - 2$ variables of type E^l_ν and $2p-2$ variables of type E^i_ν for all $i \in \{j, j+1, \dots, l-1\}$. Using Lemma 27, the variables of type E^l_ν can be contracted to

$$\begin{aligned}
&\left\lceil \frac{2p^{\tau-l+1} + (4-2m)\,p^{\tau-l} - \frac{p-1}{2} \sum_{i=1}^{\tau-l-1} p^i + (2m-1)\,p^{\tau-l-1} + 3\sum_{i=1}^{\tau-l-2} p^i - 2p + 1}{p} \right\rceil - 2p + \frac{p-3}{2} \\
&= 2p^{\tau-l} + (4-2m)\,p^{\tau-l-1} - \frac{p-1}{2} \sum_{i=0}^{\tau-l-2} p^i + (2m-1)\,p^{\tau-l-2} + 3 \sum_{i=0}^{\tau-l-3} p^i - 1 - 2p + \frac{p-3}{2} \\
&= 2p^{\tau-(l+1)+1} + (4-2m)\,p^{\tau-(l+1)} - \frac{p-1}{2} \sum_{i=1}^{\tau-(l+1)-1} p^i + (2m-1)\,p^{\tau-(l+1)-1} + 3 \sum_{i=0}^{\tau-(l+1)-2} p^i - 2p - 2
\end{aligned}$$

variables of type E^{l+1}_ν, while leaving at least $6p-9 \geq 2p-2$ variables of type E^l_ν unused. Hence, by induction, one can contract the E^j_ν variables to

$$\begin{aligned}
2p^{\tau-(\tau-1)+1} + (4-2m)\,p^{\tau-(\tau-1)} - \frac{p-1}{2} \sum_{i=1}^{\tau-(\tau-1)-1} p^i + (2m-1)\,p^{\tau-(\tau-1)-1} + 3 \sum_{i=0}^{\tau-(\tau-1)-2} p^i - 2p - 2 \\
= 2p^2 + (2-2m)\,p + 2m - 3
\end{aligned}$$

variables of type $E_\nu^{\tau-1}$ and $2p-2$ variables of type E_ν^i for all $i \in \{j, j+1, \dots, \tau-2\}$. This reduced the cases $j \leq \tau-2$ to the case $j = \tau-1$. For $j = \tau-1$, one can contract the variables of type $E_\nu^{\tau-1}$ to

$$\left\lceil \frac{2p^2 + (2-2m)\,p + 2m - 3}{2p-2} \right\rceil - 4 = p - m - 1$$

variables of type E_ν^τ with Lemma 26, while leaving at least $6p-9 \geq 2p-2$ variables of type $E_\nu^{\tau-1}$. This proves the claim. □

Lemma 35. *Let $p = 5$ and $m \leq p-1$ be an integer. Let there be*

$$3p^{\tau-j+1} - mp^{\tau-j} - 3p^{\tau-j} - \sum_{i=0}^{\tau-j-1} p^i - 2p + 2$$

variables of type E_ν^j for some $j \in \{0, 1, \dots, \tau\}$. Then one can contract them to $p-m-1$ variables of type E_ν^τ and $2p-2$ variables of type E_ν^i for all $i \in \{j, j+1, \dots, \tau-1\}$.

Proof. One can assume that $j \in \{0, 1, \dots, \tau-1\}$, because the claim is trivial for $j = \tau$.

For $j \leq \tau-2$, assume that for some $l \in \{j, j+1 \dots, \tau-2\}$ one can contract the variables to $3p^{\tau-l+1} - mp^{\tau-l} - 3p^{\tau-l} - \sum_{i=0}^{\tau-l-1} p^i - 2p + 2$ variables of type E_ν^l and $2p-2$ variables of type E_ν^i for all $i \in \{j, j+1, \dots, l-1\}$. Using Lemma 27 for $p = 5$, the variables of type E_ν^l can be contracted to

$$\begin{aligned}
&\left\lceil \frac{3p^{\tau-l+1} - mp^{\tau-l} - 3p^{\tau-l} - \sum_{i=0}^{\tau-l-1} p^i - 2p + 2}{p} \right\rceil - 2p + 3 \\
&= 3p^{\tau-l} - mp^{\tau-l-1} - 3p^{\tau-l-1} - \sum_{i=0}^{\tau-l-2} p^i - 2 + 1 - 2p + 3 \\
&= 3p^{\tau-(l+1)+1} - mp^{\tau-(l+1)} - 3p^{\tau-(l+1)} - \sum_{i=0}^{\tau-(l+1)-1} p^i - 2p + 2
\end{aligned}$$

variables of type E_ν^{l+1}, while leaving at least $6p-9 \geq 2p-2$ variables of type E_ν^l unused. By induction, it follows that one can contract

$$3p^{\tau-(\tau-1)+1} - mp^{\tau-(\tau-1)} - 3p^{\tau-(\tau-1)} - \sum_{i=0}^{\tau-(\tau-1)-1} p^i - 2p + 2 = 3p^2 - mp - 5p + 1$$

variables of type $E_\nu^{\tau-1}$ and $2p-2$ variables of type E_ν^i for all $i \in \{j, j+1, \dots, \tau-2\}$. This reduced the cases $j \leq \tau-2$ to the case $j = \tau-1$.

For $j = \tau-1$ one has $3p^2 - mp - 5p + 1$ variables of type E_ν^j. This is at least as big as $2p^2 - 2p + 1$ for $m \leq 2$. Thus, one can use Lemma 27 for $p = 5$ to contract them to

$$\left\lceil \frac{3p^2 - mp - 5p + 1}{p} \right\rceil - 2p + 3 = 3p - m - 5 + 1 - 2p + 3 = p - m - 1$$

variables of type E_ν^τ while leaving at least $2p-2$ variables of type $E_\nu^{\tau-1}$ unused. For $m = 4$ the claim follows because $p - 4 - 1 = 0$, which leaves $3p^2 - 4p - 5p + 1 = 6p + 1 \geq 2p - 2$ variables of

type $E_\nu^{\tau-1}$. In the remaining case $m = 3$, one obtains

$$\left\lceil \frac{3p^2 - 3p - 5p + 1}{2p - 2} \right\rceil - 4 = 1 = p - 3 - 1 = p - m - 1$$

variables of type E_ν^τ with Lemma 26 while leaving at least $6p - 9 \geq 2p - 2$ variables of type $E_\nu^{\tau-1}$ unused. □

Lemma 36. *Let there be* $4p^{\tau-j} - \frac{p-1}{2}\sum_{i=1}^{\tau-j-1} p^i + 3\sum_{i=0}^{\tau-j-2} p^i - 2p - 2$ *variables of type* E_ν^j *for some* $j \in \{0, 1, \ldots, \tau - 1\}$. *Then one can contract* $2p - 2$ *variables of type* E_ν^i *for all* $i \in \{j, \ldots, \tau - 1\}$, *simultaneously.*

Proof. For $j = \tau - 1$ the statement is trivial, thus, the cases $j \in \{0, 1, \ldots, \tau - 2\}$ remain. Assume that for some $l \in \{j, \ldots, \tau - 2\}$ one can contract the variables of type E_ν^j to $2p - 2$ variables in E_ν^i for all $i \in \{j, \ldots, l - 1\}$ and $4p^{\tau-l} - \frac{p-1}{2}\sum_{i=1}^{\tau-l-1} p^i + 3\sum_{i=0}^{\tau-l-2} p^i - 2p - 2$ variables of type E_ν^l. Then they can be contracted with Lemma 27 to

$$\begin{aligned}
&\left\lceil \frac{4p^{\tau-l} - \frac{p-1}{2}\sum_{i=1}^{\tau-l-1} p^i + 3\sum_{i=0}^{\tau-l-2} p^i - 2p - 2}{p} \right\rceil - 2p + \frac{p-3}{2} \\
&= 4p^{\tau-l-1} - \frac{p-1}{2}\sum_{i=0}^{\tau-l-2} p^i + 3\sum_{i=0}^{\tau-l-3} p^i - 2 + 1 - 2p + \frac{p-3}{2} \\
&= 4p^{\tau-(l+1)} - \frac{p-1}{2}\sum_{i=1}^{\tau-(l+1)-1} p^i + 3\sum_{i=0}^{\tau-(l+1)-2} p^i - 2p - 2
\end{aligned}$$

variables of type E_ν^{l+1}, while leaving at least $6p - 9 \geq 2p - 2$ variables of type E_ν^l. Via induction, one can deduce that one can contract $2p - 2$ variables of type E_ν^i for all $i \in \{j, \ldots, \tau - 2\}$ and $4p^1 - \frac{p-1}{2}\sum_{i=1}^{0} p^i + 3\sum_{i=0}^{-1} p^i - 2p - 2 = 2p - 2$ variables of type $E_\nu^{\tau-1}$. □

2.6 Pairs of Forms with $\tau = 1$

This section contains the proof that for all proper p-normalised pairs f, g with $\tau = 1$ the equations $f = g = 0$ have a non-trivial p-adic solution. This is primarily done by contracting a $C^{\tau+1} = C^2$ variable if $I_0^0 \geq p^2 + p - 1$, which indicates that the colour 0 is zero-representing, and else by contracting a $P^{\tau+1} = P^2$ variable.

The following lemma exploits p-equivalence classes by transforming some pairs f, g into p-equivalent pairs $\tilde{f}, \tilde{g}$, for which one can contract a P^2 variable.

Lemma 37. *Let* $1 \leq m \leq p$ *be a natural number and* $j \in \{0, \ldots, k - 1\}$. *Let* f, g *be a pair given by* (2.1.1) *with integer coefficients,* $\tau = 1$, $q_j \geq pm$, $m_j \geq m(2p - 1)$, $q_{j+1} \geq p - m$ *and* $I_{\max}^{j+1} \geq p - 1$. *Then there exists a non-trivial p-adic solution of* $f = g = 0$.

Proof. Apply $x \mapsto px$ for all variables at level l for all $l \in \{0, \ldots, j - 1\}$ and then multiply both equations with p^{-j}. This transforms the pair f, g into a p-equivalent pair with integer coefficients, $q_0 \geq pm$, $m_0 \geq m(2p - 1)$, $q_1 \geq p - m$ and $I_\nu^1 = I_{\max}^1 \geq p - 1$ for some ν. Using Lemma 24, one can contract the E^0 variables to m variables of type P^1. The $p - 1$ variables of type E_ν^1 and the $p - m$ variables of type E_ν^1 can be contracted together with the P^1 variables to a P^2 variable due to Lemma 23. Thus, the transformed pair has a non-trivial p-adic solution, from which it follows that the p-equivalent pair f, g has one as well. □

Due to this lemma, one can assume in the cases $q_j \geq pm$ and $m_j \geq m(2p-1)$ for some $j \in \{0, \ldots, k-1\}$ that either $q_{j+1} \leq p-m-1$ or $I_{\max}^{j+1} \leq p-2$. For a p-normalised pair, one has $m_0 \geq 2p^2 - 2p + 1 \geq (p-1)(2p-1)$ and $q_0 \geq p^2 - p + 1 \geq (p-1)p$. Therefore, one can assume that one has either $q_1 = 0$ or $I_{\max}^1 \leq p-2$. The following two lemmata divides the case $\tau = 1$ into $I_{\max}^1 \geq p-1$ and $I_{\max}^1 \leq p-2$.

Lemma 38. *Let f, g be a proper p-normalised pair with $\tau = 1$ and $I_\nu^1 = I_{\max}^1 \geq p-1$. Then the equations $f = g = 0$ have a non-trivial p-adic solution.*

Proof. As described above, one can assume that $q_1 = 0$ and thus $I_\nu^1 = I_{\max}^1 = m_1$. It follows that

$$m_0 \geq 3p^2 - 3p + 1 - q_1 = 3p^2 - 3p + 1 \geq 2p^2 - p. \tag{2.6.1}$$

Assume first that $r(f,g) = r \geq 0$. Then one can use Lemma 24 to contract the E^0 variables to p variables of type P^1 and Lemma 22 to contract the P^1 variables together with the E_ν^1 variables to a P^2 variable. Consequently, one can assume that $r = -1$, which leads to

$$I_0^0 \geq 3p^2 - 3p + 1 - q_0 - q_1 \geq 2p^2 - 3p + 2 \geq p^2 + p - 1.$$

Hence, the colour 0 is zero-representing and it suffices to show that one can contract a C^2 variable.

By Lemma 5, one knows that $\nu \in \{0, p\}$. If $\nu = p$, one can contract $2p-2$ of the variables of type E_0^0 to an E_0^1 variable, using Lemma 21 once, because $2p^2 - 3p + 2 \geq 8p - 7 = 2(4p-4) + 1$ for all $p \geq 5$. If on the other hand $\nu = 0$, one has

$$I_{00}^0 \geq \frac{I_0^0}{p} \geq 2p - 3 \geq p - 1,$$

due to Lemma 5 and

$$I_0^0 - I_{00}^0 \geq 2p^2 - 2p - q_0 - \left(m_1 - I_0^1\right) \geq p^2 - 2p + 1 \geq 1,$$

by (2.4.1). Hence, one can contract $p-1$ variables of type E_{00}^1 and one $E_{0\bar{0}}^0$ variable to an $E_{\bar{0}}^1$ variable due to Lemma 19.

In both cases, there are still at least $2p^2 - 3p + 2 - (2p-2) = 2p^2 - 5p + 4 \geq 2p - 2$ variables of type E_0^0 remaining. Those contract with $p^2 - p$ of the C^0 variables to $p-1$ variables of type C^1 due to Lemma 33. All in all, one has $p-1$ variables of type E_ν^1, one $E_{\bar{\nu}}^1$ variable and $p-1$ variables of type C^1. By Lemma 23, these can be contracted to a C^2 variable, which completes the proof. □

Lemma 39. *Let f, g be a proper p-normalised pair with $\tau = 1$ and $I_\nu^1 = I_{\max}^1 \leq p-2$. Then the equations $f = g = 0$ have a non-trivial p-adic solution.*

Proof. By $I_\mu^1 \leq I_{\max}^1 \leq p-2$ for all $0 \leq \mu \leq p$, it follows that

$$m_1 \leq (p-2)(p+1) = p^2 - p - 2.$$

If one has $q_1 \geq p$ and $m_1 \geq 2p-1$, one can assume, due to Lemma 37, that either $q_2 \leq p-2$ or

$I^2_{\max} \leq p-2$. For $q_2 \leq p-2$ it follows that

$$m_0 \geq 5p^2 - 5p + 1 - p^2 + p + 2 - p + 2 = 4p^2 - 5p + 5 \geq 4p^2 - 6p + 3,$$

while for $I^2_{\max} \leq p-2$ it follows that $m_2 \leq p^2 - p - 2$ and thus

$$m_0 \geq 6p^2 - 6p + 1 - p^2 + p + 2 - p^2 + p + 2 = 4p^2 - 4p + 5 \geq 4p^2 - 6p + 3.$$

Else, one has either $q_1 \leq p-1$ or $m_1 \leq 2p-2$. If $q_1 \leq p-1$ it follows that $m_1 \leq 2p-2$ as well, because $m_1 = I^1_{\max} + q_1$. Then one obtains

$$m_0 \geq 4p^2 - 4p + 1 - 2p + 2 = 4p^2 - 6p + 3.$$

One of these three bounds holds in any case, thus, one can assume that

$$m_0 \geq 4p^2 - 6p + 3. \tag{2.6.2}$$

This lower bound for m_0 leads to

$$I^0_0 = m_0 - q_0 \geq 4p^2 - 6p + 3 - p^2 - (r+1)\,p + 1 = 3p^2 - rp - 7p + 4. \tag{2.6.3}$$

For $r \leq p-2$ this is at least as big as $p^2 + p - 1$ for $p \geq 5$, hence, it suffices to contract a C^2 variable, whereas one has to contract a P^2 variable for $r = p-1$. The remaining proof is divided into three cases, based on the value of $r = r(f,g)$.

Case $\mathbf{r = p-1}$. If $m_0 \geq (2p-1)(2p-1) = 4p^2 - 4p + 1$, one can use Lemma 24 to contract the E^0 variables to $2p-1$ variables of type P^1. By Lemma 15, it follows that one can contract those P^1 variables to a P^2 variable. Hence, one can assume that $m_0 \leq 4p^2 - 4p$ and thus $m_1 \geq 1$. Due to (2.6.2) one has $m_0 \geq 4p^2 - 6p + 2 = (2p-1)(2p-2)$. Therefore, Lemma 24 shows that one can contract the E^0 variables to $2p-2$ variables of type P^1. Lemma 10 with $n = 2$ shows that one can contract them together with one of the E^1 variables to a variable of a level at least 2. This contraction cannot contain only the E^1 variable, thus the resulting variable has to be a P^2 variable.

Case $\mathbf{0 \leq r \leq p-2}$. One can assume that $I^1_\nu = I^1_{\max} \leq p-r-2$, because else, Lemma 33 can be used to contract $p^2 + rp$ of the C^0 variables together with $2p-2$ variables of type E^0_0 to $p+r$ variables of type C^1. Then one can contract them together with the E^1_ν variables to a C^2 variable, using Lemma 22. It follows that that

$$m_1 \leq p^2 - (r+1)\,p - r - 2. \tag{2.6.4}$$

If $q_2 \geq p-1$ and $I^2_{\max} \geq p-1$, one can use Lemma 17 to contract $p(p-r-1)$ of the variables of type E^0_0 to $p-r-1$ variables of type E^1. This is possible, because afterwards, there are still at least

$$3p^2 - rp - 7p + 4 - p(p-r-1) = 2p^2 - 6p + 4 \geq 3p - 2$$

of the E^0_0 variables unused. Lemma 33 can be used to contract $p^2 + rp$ of the C^0 and $2p-2$ of the remaining E^0_0 variables to $p+r$ variables of type C^1. One can assume that the C^1

variables are of type E^1, because else one already has a C^2 variable. Take the set $\mathscr{K}$ of the $2p-1$ variables of type E^1 that were contracted, from which $p+r$ are of type C^1. If there is a μ with $I_\mu(\mathscr{K}) \geq p$ there are at least p variables of type E^1_μ in $\mathscr{K}$. As $p+r$ of the variables in $\mathscr{K}$ are of type C^1, it follows that there is at least one C^1_μ variable in $\mathscr{K}$. Thus, one can contract the E^1_μ variables in $\mathscr{K}$ with Lemma 20 to a C^2 variable. Else, one has $q(\mathscr{K}) \geq p$ and thus, one has transformed the pair f, g into another one with $m_1 \geq 2p-1$ and $q_1 \geq p$. This new pair has the same values for q_2 and $I^2_{\max}$, thus it follows from Lemma 37 that it has a non-trivial p-adic solution. Consequently the pair f, g has one as well. Thus, one can assume that either $q_2 \leq p-2$ or $I^2_{\max} \leq p-2$.

By (2.6.4), it follows for $q_2 \leq p-2$ that

$$m_0 \geq 5p^2 - 5p + 1 - p^2 + (r+1)p + r + 2 - p + 2 = 4p^2 - 5p + rp + 5 + r$$

and for $I^2_{\max} \leq p-2$ that $m_2 \leq p^2 - p - 2$ and, therefore,

$$m_0 \geq 6p^2 - 6p + 1 - p^2 + (r+1)p + r + 2 - p^2 + p + 2 = 4p^2 - 4p + rp + 5 + r.$$

In both cases, one obtains the lower bound

$$m_0 \geq 4p^2 - 5p + rp + 5 + r,$$

which leads to

$$I^0_0 = m_0 - q_0 \geq 3p^2 - 6p + 6 + r \geq 2p^2 - 2rp + 2r - 1.$$

Now one can distinguish between the cases $m_1 \geq 1$ and $m_1 = 0$.

Case $m_1 \geq 1$**.** One can use Lemma 26 to contract the E^0_0 variables to

$$\left\lceil \frac{2p^2 - 2rp + 2r - 1}{2p-2} \right\rceil - 4 = p - r - 2$$

variables of type E^1_0. This leaves at least $6p - 9 \geq 2p - 2$ variables of type E^0_0. Hence, one can use Lemma 33 to contract them with $p^2 + rp$ of the C^0 variables to $p+r$ variables of type C^1. A set $\mathscr{H}$ containing the $p-r-2$ variables of type E^1_0, the $p+r$ variables of type C^1 and one further E^1 variables, which exists due to $m_1 \geq 1$, contains a contraction to a C^2 variable. If none of the C^1 variables is already of type C^2, there is either a μ such that $I_\mu(\mathscr{H}) \geq p$ or $q(\mathscr{H}) \geq p$. If $I_\mu(\mathscr{H}) \geq p$, then at least one of the E^1_μ variables in $\mathscr{H}$ is a C^1 variable and thus $\mathscr{H}$ contains a contraction to a C^2 variable due to Lemma 20. If on the other hand $q(\mathscr{H}) \geq p$, then $\mathscr{H}$ contains a contraction to a variable at level at least 2, which can be traced back to at least two variables of different colour at level 1, due to Lemma 14. The only way that such a variable is not of type C^2, is that the contraction contains no C^1 variable. The variables in $\mathscr{H}$ which are not of type C^1 are $p-r-2$ variables of type E^1_0 and one E^1 variable. As the contracted variable can be traced back to two variables of different colours at level 1, the E^1 variable has to be an $E^1_{\tilde{0}}$ variable. But if a subset $\mathscr{K}$ of $\mathscr{H}$ contains this variable and additionally only variables of type E^1_0, then it cannot be a contraction to a variable at level at least 2, because then one has exactly one $i \in \mathscr{K}$ for which the second entry $\tilde{b}_i$ of the level coefficient vector is not congruent to 0 modulo p. Therefore, one cannot solve

$\sum_{j\in\mathscr{K}} \tilde{b}_j y_j^k \equiv 0 \bmod p$ with all $y_j \not\equiv 0 \bmod p$. Consequently, this cannot occur, and the resulting variable is a C^2 variable.

Case $m_1 = 0$**.** This leads to the even better bound

$$m_0 \geq 4p^2 - 4p + 1$$

and thus

$$I_0^0 \geq 4p^2 - 4p + 1 - p^2 - (r+1)\,p + 1 = 3p^2 - (5+r)\,p + 2.$$

For $p \geq 7$, this is at least as big as $2p^2 + 2p - 2rp + 2r - 3$, thus, one can use Lemma 34 to contract the E_0^0 variables to $p - r - 1$ variables of type E_0^1, while leaving at least $2p-2$ variables of type E_0^0 unused. For $p = 5$, this is at least as big as $3p^2 - rp - 5p + 1$, thus Lemma 35 shows that one can contract the E_0^0 variables to $p - r - 1$ variables of type E_0^1 as well, while leaving at least $2p - 2$ variables of type E_0^0 unused. In both cases, one can use Lemma 33 to contract the $2p - 2$ variables of type E_0^0 with $p^2 + rp$ of the C^0 variables to $p + r$ variables of type C^1. Then one can contract them together with the $p - r - 1$ variables of type E_0^1 to a C^2 variable due to Lemma 22.

Case r = −1. Note first that one has $m_1 - I_0^1 \leq p^2 - 2p = (p-2)\,p$ due to $I_{\max}^1 \leq p-2$, and thus

$$I_0^0 - I_{00}^0 \geq 2p^2 - 2p - q_0 - \left(m_1 - I_0^1\right) \geq 1,$$

by (2.4.1). If $m_0 \geq 4p^2 - 4p$, one obtains the lower bound

$$I_0^0 \geq 3p^2 - 4p + 1$$

and, consequently, it follows that

$$I_{00}^0 \geq \frac{I_0^0}{p} \geq 3p - 4 \geq p - 1.$$

Therefore, one can take $p-1$ variables of type E_{00}^0 and one of type $E_{0\bar{0}}^0$ to contract a $E_{\bar{0}}^1$ variable by Lemma 19. There are at least $3p^2 - 5p + 1$ variables of type E_0^0 remaining, which can be contracted to $p-1$ variables of type E_0^1 using Lemma 26 for $p \geq 7$ and Lemma 27 for $p = 5$. This leaves at least $6p - 9 \geq 2p - 2$ variables of type E_0^0, which can be contracted with $p^2 - p$ of the C^0 variables to $p-1$ variables of type C^1 using Lemma 33. Then one can use Lemma 23 to contract the $p-1$ variables of type E_0^1, the $p-1$ variables of type C^1 and the $E_{\bar{0}}^1$ variable to a C^2 variable. Hence, one can assume that

$$m_0 \leq 4p^2 - 4p - 1.$$

It follows that $m_1 \geq 2$. Note that one has

$$I_0^0 \geq 3p^2 - 6p + 4 \geq 2p^2 - 1 = (2p-2)\,(p+1) + 1 \quad \text{and} \quad I_{00}^0 \geq 3p - 6 \geq p - 1$$

due to (2.6.3).

Case $m_1 - I_0^1 = 0$**.** Due to $m_1 \geq 2$, one has $I_0^1 \geq 2$. Take a set which contains $p-1$ variables of type E_{00}^0 and one $E_{0\bar{0}}^0$ variable. This set contains a contraction to an $E_{\bar{0}}^1$ variable due to Lemma 19. Then there are at least $3p^2 - 7p + 4 \geq 2p^2 - 2p + 1$ variables of type E_0^0 left. Therefore, one can use Lemma 26 to contract them to $p-3$ variables of type E_0^1, giving a total of $p-1$, while leaving at least $6p - 9 \geq 2p - 2$ variables of type E_0^0 unused. Lemma 33 can be used to contract $2p-2$ of the remaining E_0^0 variables together with $p^2 - p$ of the C^0 variables to $p-1$ variables of type C^1. One can contract the $p-1$ variables of type E_0^1, the $E_{\bar{0}}^1$ variable and the $p-1$ variables of type C^1 to a C^2 variable, due to Lemma 23.

Case $m_1 - I_0^1 \geq 1$**.** Use Lemma 26 to contract the E_0^0 variable to $p-2$ variables of type E_0^1, while leaving at least $6p - 9 \geq 2p - 2$ unused. Then one can take Lemma 33 to contract $p^2 - p$ of the C^0 variables together with $2p-2$ of the remaining E_0^0 variables to $p-1$ variables of type C^1. If $I_0^1 \geq 1$, then one can use Lemma 23 to contract the $p-1$ variables of type E_0^1, the $p-1$ variables of type C^1 and one of the $E_{\bar{0}}^1$ variables to a C^2 variable. Thus, one can assume that $I_0^1 = 0$, $m_1 - I_0^1 \geq 2$ and

$$m_1 \leq p^2 - 2p,$$

because $I_{\max}^1 \leq p-2$. If none of the C^1 variable is already of type C^2, they are all E^1 variables. Take a set $\mathscr{K}$ containing the C^1 variables, two of the $E_{\bar{0}}^1$ variables which exist due to $m_1 - I_0^1 \geq 2$ and the $p-2$ variables of type E_0^1. If there is a μ such that $I_\mu(\mathscr{K}) \geq p$, then there is at least one C_μ^1 variable in $\mathscr{K}$. By Lemma 20, one can contract the variables in $\mathscr{K}$ of colour μ to a C^2 variable. Else, one has $q(\mathscr{K}) \geq p$, because $|\mathscr{K}| = 2p-1$. It follows that one has transformed the pair f, g into a pair with $m_1 \geq 2p-1$ and $q_1 \geq p$. The new pair either has a non-trivial p-adic solution due to Lemma 37, from which it would follow that f, g has one as well, or it has $q_2 \leq p-2$ or $I_{\max}^2 \leq p-2$. As the new pair has the same parameter q_2 and $I_{\max}^2$ as the pair f, g, one can assume that $q_2 \leq p-2$ or $I_{\max}^2 \leq p-2$ holds for f, g as well. This contradicts the p-normalisation, because then one of the inequalities

$$m_0 + m_1 + q_2 \leq 4p^2 - 4p - 1 + p^2 - 2p + p - 2 = 5p^2 - 5p - 3 < 5p^2 - 5p + 1,$$

and

$$m_0 + m_1 + m_2 \leq 4p^2 - 4p - 1 + p^2 - 2p + p^2 - p - 2 = 6p^2 - 7p - 3 < 6p^2 - 6p + 1,$$

holds, hence, it follows that this case cannot occur.

This concludes the case $r = -1$ and with that the claim follows. □

This shows that for every proper p-normalised pair f, g the equations $f = g = 0$ have a non-trivial p-adic solution provided that $\tau = 1$.

2.7 Pairs of Forms with $\tau \geq 2$

This section contains the proof of the theorem for $\tau \geq 2$, which completes the proof. In general, the proof relies on the same techniques independent on the actual value of τ, but sometimes one has to separate the cases $\tau = 2$ and $\tau = 3$, because the proof is easier for bigger τ and, hence, the cases $\tau \in \{2, 3\}$ require some extra effort.

In order to avoid a repetition of the same argument, the following lemma points out a situation in which one can contract a $C^{\tau+1}$ or a $P^{\tau+1}$ variable, which appears constantly in the proof for $\tau \geq 2$.

Lemma 40. *Let $S \in \{C, P\}$ and $0 \leq m \leq p-1$. Let there be $p^{\tau-j+1} + mp^{\tau-j}$ variables of type S^j for some $j \in \{0, \dots, \tau-1\}$ and $p-m-1$ variables of type E^τ_ν for some ν. Furthermore, for $i \in \{j, j+1, \dots, \tau-1\}$ let there be $2p-2$ variables of type $E^i_{\nu_i}$ for some colours ν_i. Then one can contract them to a variable of type $S^{\tau+1}$.*

Proof. One can contract the variables of type S^j and type $E^i_{\nu_i}$ for $i \in \{j, \dots, \tau-1\}$ to $p+m$ variables at level of type S^τ due to Lemma 33. Those and the $p-m-1$ variables of type E^τ_ν can be contracted to a variable of type $S^{\tau+1}$ using Lemma 22. □

The following lemma focuses on cases, where the number of variables at level 0 is small.

Lemma 41. *Let f, g be a proper p-normalised pair with $\tau \geq 2$ and $m_0 \leq 3p^{\tau+1} - 4p^\tau - 2p^{\tau-1} + p + 3$. Then the equations $f = g = 0$ have a non-trivial p-adic solution.*

Proof. By the p-normalisation of f, g, one has $q_0 \geq p^{\tau+1} - p^\tau + 1$ and $m_0 \geq 2p^{\tau+1} - 2p^\tau + 1$, from which it follows that one can contract the variables at level 0 to $p^\tau - p^{\tau-1}$ variables of type P^1 due to Lemma 24. The upper bound of m_0 provides the bounds

$$\begin{aligned} m_1 &\geq 4p^{\tau+1} - 4p^\tau + 1 - 3p^{\tau+1} + 4p^\tau + 2p^{\tau-1} - p - 3 \\ &= p^{\tau+1} + 2p^{\tau-1} - p - 2 \geq 2p^\tau + 4p^{\tau-1} + p^2 - p - 7 \\ &= \left(p^{\tau-1} + 3 \sum_{i=0}^{\tau-2} p^i - 1 \right) (2p-2) + p^2 - 5p - 3 \end{aligned}$$

and

$$\begin{aligned} q_1 &\geq 3p^{\tau+1} - 3p^\tau + 1 - 3p^{\tau+1} + 4p^\tau + 2p^{\tau-1} - p - 3 \\ &= p^\tau + 2p^{\tau-1} - p - 2 = \left(p^{\tau-1} + 3 \sum_{i=0}^{\tau-2} p^i - 1 \right) (p-1) \,. \end{aligned}$$

Therefore, there are at least $\left(p^{\tau-1} + 3\sum_{i=0}^{\tau-2} p^i - 1\right)(2p-2) + p^2 - 3p + 1$ variables of type E^1 from which at least $\left(p^{\tau-1} + 3\sum_{i=0}^{\tau-2} p^i - 1\right)(p-1)$ are of type E^1_ν for all $0 \leq \nu \leq p$. Those variables can be contracted together with the P^1 variables to $2p^{\tau-1} + p^{\tau-2} - 2$ variables of type P^2 by using Lemma 30 with $x = p^{\tau-1} - 2p^{\tau-2} - 3\sum_{i=0}^{\tau-3} p^i - 1$, $y = p^{\tau-1} + 3\sum_{i=0}^{\tau-2} p^i - 1$ and $z = p-2$. Then Lemma 32 can be used to contract the P^2 variables to $2p-1$ variables of type P^τ, which contract to a $P^{\tau+1}$ variable due to Lemma 15. □

For bigger m_0 it is helpful to divide the cases depending on the value of $r(f, g)$. The following three lemmata completes the proof that a for a proper p-normalised pair f, g with $\tau \geq 2$ and $r = r(f, g) \geq 0$ the equations $f = g = 0$ have a non-trivial p-adic solution.

This is done by using different strategies depending on the size of m_0. The area of the value of m_0 in which one has to use a certain strategy differs between $p \geq 7$ and $p = 5$. This is due to some inequalities, which do not hold if p is too small. To counter this, the lemmata that are stronger in the case $p = 5$ are used, which results in the different areas.

Lemma 42. *Let f, g be a proper p-normalised pair with $\tau \geq 2$, $r = r(f,g) \geq 0$ and $m_0 \geq 3p^{\tau+1} + 8p^{\tau}$ for $p \geq 7$ and $m_0 \geq 3p^{\tau+1} + 3p^{\tau}$ for $p = 5$. Then the equations $f = g = 0$ have a non-trivial p-adic solution.*

Proof. As $I_0^0 = m_0 - q_0$, one can estimate I_0^0 via

$$I_0^0 = m_0 - q_0 \geq 3p^{\tau+1} + 8p^{\tau} - p^{\tau+1} - (r+1)\,p^{\tau} + 1 = 2p^{\tau+1} + (7-r)\,p^{\tau} + 1,$$

for all primes $p \geq 7$, and via

$$I_0^0 = m_0 - q_0 \geq 3p^{\tau+1} + 3p^{\tau} - p^{\tau+1} - (r+1)\,p^{\tau} + 1 = 2p^{\tau+1} + (2-r)\,p^{\tau} + 1,$$

for $p = 5$. Both are at least as big as $p^{\tau+1} + p^{\tau} - 1$, because $r \leq p-1$, from which it follows that the colour 0 is zero-representing, and, hence, it suffices to contract a $C^{\tau+1}$ variable. Furthermore, the lower bound for I_0^0 implies that

$$I_0^0 \geq 2p^{\tau+1} + (4-2r)\,p^{\tau} + (2r-1)\,p^{\tau-1} + 3\sum_{i=0}^{\tau-2} p^i - 2p - 2$$

for $p \geq 7$ and

$$I_0^0 \geq 3p^{\tau+1} - rp^{\tau} - 3p^{\tau} - \sum_{i=0}^{\tau-1} p^i - 2p + 2$$

for $p = 5$. Thus, one can contract the E_0^0 variables to $p - r - 1$ variables of type E_0^{τ}, using Lemma 34 for $p \geq 7$ and Lemma 35 for $p = 5$, while leaving at least $2p-2$ variables of type E_0^i for all $i \in \{0, 1, \ldots, \tau-1\}$. Then one can contract $p^{\tau+1} + rp^{\tau}$ variables of type C^0 together with the $2p-2$ variables of type E_0^i for all $i \in \{0, 1, \ldots, \tau-1\}$ and the E_0^{τ} variables to a $C^{\tau+1}$ variable due to Lemma 40. □

Lemma 43. *Let f, g be a proper p-normalised pair f, g with $\tau \geq 2$, $r = r(f,g) \geq 0$, and $m_0 \geq 3p^{\tau+1} + p^{\tau} - 3$ which has $m_0 \leq 3p^{\tau+1} + 8p^{\tau} - 1$ for $p \geq 7$ and $m_0 \leq 3p^{\tau+1} + 3p^{\tau} - 1$ for $p = 5$. Then the equations $f = g = 0$ have a non-trivial p-adic solution.*

Proof. By $q_0 \leq 2p^{\tau+1} - 2$, one obtains

$$I_0^0 = m_0 - q_0 \geq 3p^{\tau+1} + p^{\tau} - 3 - 2p^{\tau+1} + 2 = p^{\tau+1} + p^{\tau} - 1,$$

from which it follows that the colour 0 is zero-representing. Therefore, it suffices to contract a $C^{\tau+1}$ variable. The variables of type E_0^0 can be contracted with Lemma 36 to $2p-2$ variables of type E_0^i for all $i \in \{0, 1, \ldots, \tau-1\}$ as

$$I_0^0 \geq p^{\tau+1} + p^{\tau} - 1 \geq 4p^{\tau} - \frac{p-1}{2}\sum_{i=1}^{\tau-1} p^i + 3\sum_{i=0}^{\tau-2} p^i - 2p - 2.$$

If $I_{\nu}^{\tau} \geq p - r - 1$ for some ν, then one can contract the $p^{\tau+1} + rp^{\tau}$ variables of type C^0 together with the $p-r-1$ variables of type E_{ν}^{τ} and the $2p-2$ variables of type E_0^i for all $i \in \{0, \ldots, \tau-1\}$ to one variable of type $C^{\tau+1}$ with Lemma 40. Thus one can assume that

$$m_{\tau} \leq (p-r-2)\,(p+1) = p^2 - (r+1)\,p - r - 2 \leq p^2. \tag{2.7.1}$$

Likewise, if $I_\nu^j \geq 2p^{\tau-j+1} + (4-2r)\,p^{\tau-j} - \frac{p-1}{2}\sum_{i=1}^{\tau-j-1} p^i + (2r-1)\,p^{\tau-j-1} + 3\sum_{i=0}^{\tau-j-2} p^i - 2p - 2$ for some $j \in \{1,\dots,\tau-1\}$ and some ν, one can contract the variables of type E_ν^j to $p-r-1$ variables of type E_ν^τ due to Lemma 34. Then again, one can contract the $p^{\tau+1} + rp^\tau$ variables of type C^0 together with the $p-r-1$ variables of type E_ν^τ and the $2p-2$ variables of type E_0^i for all $i \in \{0,\dots,\tau-1\}$ to a $C^{\tau+1}$ variable with Lemma 40. Hence, one can assume that this is not the case, giving the upper bound

$$I_{\max}^j \leq 2p^{\tau-j+1} + (4-2r)\,p^{\tau-j} - \frac{p-1}{2}\sum_{i=1}^{\tau-j-1} p^i + (2r-1)\,p^{\tau-j-1} + 3\sum_{i=0}^{\tau-j-2} p^i - 2p - 3. \tag{2.7.2}$$

If $m_j \geq 2p^{\tau-j+1} - (2r+2)\,p^{\tau-j} + p^2 - 3p + 2r + 1$ and $q_j \geq p^{\tau-j+1} - (r+1)\,p^{\tau-j} + r$ for some $j \in \{1,\dots,\tau-1\}$, one can contract $p^{\tau+1} + rp^\tau$ of the C^0 variables together with the $2p-2$ variables of type E_0^i for $i \in \{0,\dots,j-1\}$ to $p^{\tau-j+1} + rp^{\tau-j}$ variables of type C^j, using Lemma 33. It follows from the lower bounds for m_j and q_j that one can contract the variables of type E^j together with the $p^{\tau-j+1} + rp^{\tau-j}$ variables of type C^j to $2p^{\tau-j} - p^{\tau-j-1} - 1$ variables of type C^{j+1}, using Lemma 30 with $x = p^{\tau-j} - p^{\tau-j-1} + r\sum_{i=0}^{\tau-j-1} p^i$, $y = p^{\tau-j} - r\sum_{i=0}^{\tau-j-1} p^i$ and $z = r$. This leaves at least $p+r$ of the C^j variables unused. Furthermore, the $2p-2$ variables of type E_0^j which were contracted at the beginning of the proof are unused as well. Hence, Lemma 22 can be used to contract $p-1$ of them and p of the remaining C^j variables to another C^{j+1} variable. All in all, one has $2p^{\tau-j} - p^{\tau-j-1}$ variables of type C^{j+1} and $2p-2$ variables of type E_0^i for all $i \in \{j+1,\dots,\tau-1\}$ left. By Lemma 40, these variables contract to a $C^{\tau+1}$ variable. One can therefore assume that either $m_j \leq 2p^{\tau-j+1} - (2r+2)\,p^{\tau-j} + p^2 - 3p + 2r$ or $q_j \leq p^{\tau-j+1} - (r+1)\,p^{\tau-j} + r - 1$ for $j \in \{1,\dots,\tau-1\}$. It follows that either one has $m_j \leq 2p^{\tau-j+1} - (2r+2)\,p^{\tau-j} + p^2 - 3p + 2r$ or for $q_j \leq p^{\tau-j+1} - (r+1)\,p^{\tau-j} + r - 1$ one obtains, due to (2.7.2), the upper bound

$$m_j \leq 3p^{\tau-j+1} + (3-3r)\,p^{\tau-j} - \frac{p-1}{2}\sum_{i=1}^{\tau-j-1} p^i + (2r-1)\,p^{\tau-j-1} + 3\sum_{i=0}^{\tau-j-2} p^i - 2p + r - 4.$$

Both upper bounds are smaller than $4p^{\tau-j+1}$, thus one can assume that $m_j \leq 4p^{\tau-j+1}$ for $j \in \{1,\dots,\tau-1\}$. It follows that one has $m_1 \leq 4p^\tau$ for all $\tau \geq 2$ and $m_2 \leq 4p^{\tau-1} \leq p^\tau$ for $\tau \geq 3$. Furthermore, one has $m_2 \leq p^\tau$ for $\tau = 2$ due to (2.7.1). It follows that

$$m_0 + m_1 + m_2 \leq 3p^{\tau+1} + 13p^\tau - 1 \leq 6p^{\tau+1} - 6p^\tau$$

for all $p \geq 7$, whereas one obtains

$$m_0 + m_1 + m_2 \leq 3p^{\tau+1} + 8p^\tau - 1 \leq 6p^{\tau+1} - 6p^\tau$$

for $p = 5$. This contradicts the p-normalisation of f, g, from which the claim follows. □

Lemma 44. *Let f, g be a proper p-normalised pair with $\tau \geq 2$, $r = r(f,g) \geq 0$ and $3p^{\tau+1} - 4p^\tau - 2p^{\tau-1} + p + 4 \leq m_0 \leq 3p^{\tau+1} + p^\tau - 4$. Then the equations $f = g = 0$ have a non-trivial p-adic solution.*

Proof. By Lemma 24, $r \geq 0$ and $m_0 \geq 2p^{\tau+1} - p^\tau$, one can contract the E^0 variables to p^τ variables of type P^1.

If there is a ν such that $I_\nu^1 \geq 2p^\tau + 4p^{\tau-1} - \frac{p-1}{2}\sum_{i=1}^{\tau-2} p^i - p^{\tau-2} + 3\sum_{i=0}^{\tau-3} p^i - 2p - 2$, one can contract the variables of type E_ν^1 with Lemma 34 and the resulting variables together with

the variables of type P^1 to a variable of type $P^{\tau+1}$ with Lemma 40. From now on, one can assume that

$$I^1_\nu \leq 2p^\tau + 4p^{\tau-1} - \frac{p-1}{2}\sum_{i=1}^{\tau-2} p^i - p^{\tau-2} + 3\sum_{i=0}^{\tau-3} p^i - 2p - 3$$

for all ν.

If $m_1 \geq 3p^\tau + 5p^{\tau-1} - \frac{p-1}{2}\sum_{i=1}^{\tau-2} p^i - p^{\tau-2} + 3\sum_{i=0}^{\tau-3} p^i - 3p - 4$, it follows, therefore, that

$$q_1 = m_1 - I^1_{\max} \geq p^\tau + p^{\tau-1} - p - 1 = \left(p^{\tau-1} + 2\sum_{i=0}^{\tau-2} p^i - 1\right)(p-1)$$

and

$$m_1 \geq 2p^\tau + 2p^{\tau-1} + p^2 - 5p - 1 = \left(p^{\tau-1} + 2\sum_{i=0}^{\tau-2} p^i - 1\right)(2p-2) + p^2 - 3p + 1.$$

Hence, one can use Lemma 30 with $x = p^{\tau-1} - p^{\tau-2} - 2\sum_{i=0}^{\tau-3} p^i - 1$, $y = p^{\tau-1} + 2\sum_{i=0}^{\tau-2} p^i - 1$ and $z = p-1$ to contract the E^1 variables together with the P^1 variables to obtain $2p^{\tau-1} + p^{\tau-2} - 2$ variables of type P^2. Then one can contract them to $2p-1$ variables of type P^τ with Lemma 32 and these to one $P^{\tau+1}$ variable with Lemma 15. Thus, one can assume that

$$m_1 \leq 3p^\tau + 5p^{\tau-1} - \frac{p-1}{2}\sum_{i=1}^{\tau-2} p^i - p^{\tau-2} + 3\sum_{i=0}^{\tau-3} p^i - 3p - 5.$$

If one has the even stronger upper bound $m_1 \leq 2p^2 - p - 3$, the p-normalisation of f, g can be used to obtain the lower bounds

$$\begin{aligned} m_2 &\geq 6p^{\tau+1} - 6p^\tau + 1 - 3p^{\tau+1} - p^\tau + 4 - 2p^2 + p + 3 \\ &= 3p^{\tau+1} - 7p^\tau - 2p^2 + p + 8 \geq 2p^{\tau-1} + 2p^{\tau-2} + p^2 - 3p - 3 \\ &= \left(p^{\tau-2} + 2\sum_{i=0}^{\tau-3} p^i\right)(2p-2) + p^2 - 3p + 1 \end{aligned}$$

and

$$\begin{aligned} q_2 &\geq 5p^{\tau+1} - 5p^\tau + 1 - 3p^{\tau+1} - p^\tau + 4 - 2p^2 + p + 3 \\ &= 2p^{\tau+1} - 6p^\tau - 2p^2 + p + 8 \geq p^{\tau-1} + p^{\tau-2} - 2 \\ &= \left(p^{\tau-2} + 2\sum_{i=0}^{\tau-3} p^i\right)(p-1)\,. \end{aligned}$$

One can contract the P^1 variables to $p^{\tau-1} - 2$ variables of type P^2 using Lemma 32. For $\tau = 2$, one can use Lemma 29 to contract one of the P^2 variables together with the E^2 variables to a $P^3 = P^{\tau+1}$ variable, because $p^{2-2} + 2\sum_{i=0}^{2-3} p^i = 1$. For $\tau \geq 3$ on the other hand, one can use Lemma 30 with $x = p^{\tau-2} - p^{\tau-3} - 2\sum_{i=0}^{\tau-4} p^i - 1$, $y = p^{\tau-2} + 2\sum_{i=0}^{\tau-3} p^i$ and $z = p-4$ to contract the P^2 variables to $2p^{\tau-2} + p^{\tau-3} - 1$ variables of type P^3. Then one can use Lemma 32 to contract them to $2p-1$ variables of type P^τ and Lemma 15 to obtain a $P^{\tau+1}$ variable. One can therefore assume that $m_1 \geq 2p^2 - p - 2 = (2p-3)(p+1) + 1$, from which it follows that

there is a ν such that

$$I^1_\nu \geq 2p-2.$$

One can contract the p^τ variables of type P^1 together with the $2p-2$ variables of type E^1_ν to $p^{\tau-1}$ variables of type P^2 with Lemma 33. The p-normalisation of f,g can be used to obtain the lower bound

$$m_2 \geq 6p^3-6p^2+1-3p^3-p^2+4-3p^2-2p+6 = 3p^3-10p^2-2p+11 \geq p^2-p-1$$

for $\tau = 2$ and

$$\begin{aligned} m_2 &\geq 6p^{\tau+1}-6p^\tau+1-3p^{\tau+1}-p^\tau+4-3p^\tau-5p^{\tau-1}+\frac{p-1}{2}\sum_{i=1}^{\tau-2}p^i+p^{\tau-2}-3\sum_{i=0}^{\tau-3}p^i+3p+5 \\ &= 3p^{\tau+1}-10p^\tau-5p^{\tau-1}+\frac{p-1}{2}\sum_{i=1}^{\tau-2}p^i+p^{\tau-2}-3\sum_{i=0}^{\tau-3}p^i+3p+10 \\ &\geq 2p^\tau+6p^{\tau-1}+3p^{\tau-2}+2p^{\tau-3}+6\sum_{i=0}^{\tau-4}p^i \geq (p+1)\left(2p^{\tau-1}+4p^{\tau-2}-p^{\tau-3}+3\sum_{i=0}^{\tau-4}p^i\right). \end{aligned}$$

for $\tau \geq 3$. Thus, there is a μ with $I^2_\mu \geq p-1$ for $\tau = 2$ and a μ with

$$I^2_\mu \geq 2p^{\tau-1}+4p^{\tau-2}-\frac{p-1}{2}\sum_{i=1}^{\tau-3}p^i-p^{\tau-3}+3\sum_{i=0}^{\tau-4}p^i-2p-2,$$

for $\tau \geq 3$. For $\tau = 2$, one can contract the $p-1$ variables of type E^2_μ together with the p variables of type P^2 to a $P^3 = P^{\tau+1}$ variable with Lemma 22. If $\tau \geq 3$, one can obtain a $P^{\tau+1}$ by contracting the E^2_μ variables with Lemma 34 and the resulting ones together with the P^2 variables with Lemma 40. □

This completes the case $r(f,g) \geq 0$. The following three lemmata completes the case $\tau \geq 2$ by showing that for every proper p-normalised pair f,g with $\tau \geq 2$ and $r(f,g) = -1$ the equations $f = g = 0$ have a non-trivial p-adic solution. Here, it is useful to choose strategies depending on the value of I^0_0. As for $r(f,g) \geq 0$, some of the bounds differ for $p = 5$ in order to balance that some inequalities only hold for $p \geq 7$.

Lemma 45. *Let f,g be a proper p-normalised pair with $\tau \geq 2$, $r = r(f,g) = -1$, and $I^0_0 \geq 2p^{\tau+1}+\frac{11}{2}p^\tau-p^{\tau-1}+3\sum_{i=0}^{\tau-2}p^i+2p^2-\frac{11}{2}p-2$. Then the equations $f = g = 0$ have a non-trivial p-adic solution. For $p = 5$ even $I^0_0 \geq 3p^{\tau+1}-\sum_{i=0}^{\tau}p^i+2p^2-6p+2$ is sufficient.*

Proof. It is sufficient to contract a $C^{\tau+1}$ variable because $I^0_0 \geq p^{\tau+1}+p^\tau-1$ is given, which implies that the colour 0 is zero-representing. By Lemma 5, it follows that

$$I^0_{00} \geq \frac{I^0_0}{p} \geq 2p^\tau+\frac{11}{2}p^{\tau-1}-p^{\tau-2}+3\sum_{i=0}^{\tau-3}p^i+2p-\frac{11}{2}$$

for $p \geq 5$ and

$$I^0_{00} \geq 3p^\tau-\sum_{i=0}^{\tau-1}p^i+2p-6,$$

for $p = 5$, which is both bigger than $(p-1)\left(p^{\tau-1}+p-2\right) = p^{\tau}-p^{\tau-1}+p^2-3p+2$. Furthermore, by (2.4.1), one obtains

$$I_0^0 - I_{00}^0 \geq 2p^{\tau+1} - 2p^{\tau} - q_0 - \left(m_1 - I_0^1\right) \geq p^{\tau+1} - 2p^{\tau} + 1 - \left(m_1 - I_0^1\right),$$

as one has $q_0 \leq p^{\tau+1}-1$, due to $r = -1$. This is bigger than $p^{\tau-1}+p-2-\left(m_1-I_0^1\right)$, therefore, one can take $p^{\tau-1}+p-2-\left(m_1-I_0^1\right)$ sets containing one variable of type $E_{0\bar{0}}^0$ and $p-1$ variables of type E_{00}^0. By Lemma 19, each of this set contains a contraction to a $E_{\bar{0}}^1$ variable. For $p \geq 5$ there are at least

$$2p^{\tau+1} + 5p^{\tau} - \frac{p-1}{2}\sum_{i=1}^{\tau-1} p^i - p^{\tau-1} + 3\sum_{i=0}^{\tau-2} p^i + p^2 - 4p - 2$$

and for $p = 5$ at least

$$3p^{\tau+1} - 2p^{\tau} - \sum_{i=0}^{\tau-1} p^i + p^2 - 4p + 2$$

variables of type E_0^0 left, which is both at least as big as

$$p^{\tau} + 4p^2 - 6p + 1 = p\left(p^{\tau-1}+p-2\right) + 3p^2 - 4p + 1.$$

As long as there are at least $p(3p-3)+1 = 3p^2-3p+1$ variables of type E_0^0 left, one has at least $3p-2$ variables of type $E_{0\mu}^0$ for some μ. Therefore, one can use Lemma 18 to contract $p^{\tau}+p^2-2p$ of the E_0^0 variables to $p^{\tau-1}+p-2$ variables of type E_0^1, using each time p variables of the same colour nuance. Now, one has $p^{\tau-1}+p-2$ variables of type E_0^1 and $p^{\tau-1}+p-2$ variables of type $E_{\bar{0}}^1$. This leaves at least

$$2p^{\tau+1} + 4p^{\tau} - \frac{p-1}{2}\sum_{i=1}^{\tau-1} p^i - p^{\tau-1} + 3\sum_{i=0}^{\tau-2} p^i - 2p - 2$$

variables of type E_0^0 for $p \geq 5$ and

$$3p^{\tau+1} - 3p^{\tau} - \sum_{i=0}^{\tau-1} p^i - 2p + 2$$

for $p = 5$ remaining. Use Lemma 34 for $p \geq 5$ and Lemma 35 for $p = 5$ to contract the E_0^0 variables to $p-1$ variables of type E_0^{τ} and $2p-2$ variables of type E_0^i for all $i \in \{0,1,\ldots,\tau-1\}$. With Lemma 33, one can contract $p^{\tau+1}-p^{\tau}$ of the variables of type C^0 and the $2p-2$ variables of type E_0^0 to $p^{\tau}-p^{\tau-1}$ variables of type C^1. Use Lemma 28 with $x = p^{\tau-1} - \sum_{i=0}^{\tau-2} p^i - 1$, $y = \sum_{i=0}^{\tau-2} p^i + 1$ and $z = p-2$ to contract $p^{\tau-1}+p-2$ variables of type E_0^1 and $p^{\tau-1}+p-2$ variables of type $E_{\bar{0}}^1$ together with the C^1 variables to $p^{\tau-1}-1$ variables of type C^2 without using $2p-2 \geq p$ of the C^1 variables. The $2p-2 \geq p-1$ variables of type E_0^1, which where contracted while the $p-1$ variables of type E_0^{τ} were contracted, are also unused. One can contract $p-1$ of them together with p of the remaining C^1 variables to an additional C^2 variable using Lemma 22. This gives a total of $p^{\tau-1}$ variables of type C^2. Then one can contract the C^2 variables with the E_0^i variables for $i \in \{2,\ldots,\tau-1\}$ and the E_0^{τ} variables to a $C^{\tau+1}$ variable due to Lemma 40. □

Lemma 46. *Let f, g be a proper p-normalised pair with $\tau \geq 2$, $r = r(f,g) = -1$ and $p^{\tau+1} + p^\tau - 1 \leq I_0^0 \leq 2p^{\tau+1} + \frac{11}{2}p^\tau - p^{\tau-1} + 3\sum_{i=0}^{\tau-2} p^i + 2p^2 - \frac{11}{2}p - 3$ for $p \geq 7$ and $p^{\tau+1} + p^\tau - 1 \leq I_0^0 \leq 3p^{\tau+1} - \sum_{i=0}^{\tau} p^i + 2p^2 - 6p + 1$ for $p = 5$. Then the equations $f = g = 0$ have a non-trivial p-adic solution.*

Proof. It follows from $r = -1$ and the restrictions on I_0^0 that

$$m_0 \leq 3p^{\tau+1} + \frac{11}{2}p^\tau - p^{\tau-1} + 3\sum_{i=0}^{\tau-2} p^i + 2p^2 - \frac{11}{2}p - 4, \tag{2.7.3}$$

for $p \geq 7$, whereas one can obtain for $p = 5$ the even better bound

$$m_0 \leq 4p^{\tau+1} - \sum_{i=0}^{\tau} p^i + 2p^2 - 6p. \tag{2.7.4}$$

As $I_0^0 \geq p^{\tau+1} + p^\tau - 1$, the colour 0 is zero-representing, hence, it suffices to show that one can contract a $C^{\tau+1}$ variable. Due to the p-normalisation of f, g and $r = -1$, one has the lower bound

$$I_0^0 \geq 3p^{\tau+1} - 3p^\tau + 1 - q_0 - q_1 \geq 2p^{\tau+1} - 3p^\tau + 2 - q_1$$

as well.

Assume first that $I_\nu^1 = I_{\max}^1 \geq p^\tau + 4p^{\tau-1} - \frac{p-1}{2}\sum_{i=1}^{\tau-2} p^i + 3\sum_{i=0}^{\tau-3} p^i - p - 4$. Then one can make sure that, additionally, one has $p^\tau + p - 2$ variables of type $E_{\tilde{\nu}}^1$ by contracting the E_0^0 variables to at least $p^\tau + p - 2 - q_1$ variables of type $E_{\tilde{\nu}}^1$ as described in the following paragraph.

One can assume that $q_1 \leq p^\tau + p - 3$, because else, there is nothing to be done. If $\nu \neq 0$, one can contract the variables of type E_0^0 to

$$\left\lceil \frac{2p^{\tau+1} - 3p^\tau + 2 - q_1}{p} \right\rceil - 2p + \frac{p-3}{2} \geq 2p^\tau - 3p^{\tau-1} + \frac{2-q_1}{p} - 2p + \frac{p-3}{2}$$

variables of type E_0^1 with Lemma 27 for $p \geq 7$, which is at least as big as $p^\tau + p - 2 - q_1$ for $p \geq 7$ and to

$$\left\lceil \frac{2p^{\tau+1} - 3p^\tau + 2 - q_1}{p} \right\rceil - 2p + 3 \geq 2p^\tau - 3p^{\tau-1} + \frac{2-q_1}{p} - 2p + 3 \geq p^\tau + p - 2 - q_1$$

variables of type E_0^1 with Lemma 27 for $p = 5$. This leaves $6p - 9 \geq 2p - 2$ variables of type E_0^0 unused in both cases. If, on the other hand, one has $\nu = 0$, it follows that

$$I_{00}^0 \geq \frac{I_0^0}{p} \geq 2p^\tau - 3p^{\tau-1} + \frac{2-q_1}{p} \geq p^\tau + p - 2 - q_1$$

and by $m_1 - I_0^1 = q_1$ and (2.4.1) that

$$I_0^0 - I_{00}^0 \geq 2p^{\tau+1} - 2p^\tau - q_0 - q_1 \geq p^{\tau+1} - 2p^\tau + 1 - q_1 \geq p^\tau + p - 2 - q_1.$$

Furthermore, one has

$$I_0^0 \geq 2p^{\tau+1} - 3p^\tau + 2 - q_1 \geq p^{\tau+1} + 2p^2 - 5p - q_1 p + 3 = p\left(p^\tau + p - 2 - q_1\right) + p^2 - 3p + 3.$$

Thus one can contract $p^{\tau+1}+p^2-2p-q_1p$ of the E_0^0 variables to $p^\tau+p-2-q_1$ variables of type $E_{\bar{0}}^1$ due to Lemma 31, leaving at least $p^{\tau+1}-3p^\tau-p^2+2p+2+(p-1)\,q_1\geq 2p-2$ variables of type E_0^0 unused.

In both cases, one has contracted enough E_ν^1 variables to have at least $p^\tau+p-2$ variables of type $E_{\bar{\nu}}^1$, while there are $2p-2$ variables of type E_0^0 remaining. The E_0^0 variables can be contracted together with $p^{\tau+1}-p^\tau$ of the C^0 variables to $p^\tau-p^{\tau-1}$ variables of type C^1, using Lemma 33. Then one can contract $4p^{\tau-1}-\frac{p-1}{2}\sum_{i=1}^{\tau-2}p^i+3\sum_{i=0}^{\tau-3}p^i-2p-2$ of the variables of type E_ν^1 with Lemma 36 to $2p-2$ variables of type E_ν^j for all $j\in\{1,\dots,\tau-1\}$. The remaining $p^\tau+p-2$ variables of type E_ν^1 together with the $p^\tau+p-2$ variables of type $E_{\bar{\nu}}^1$ and the C^1 variables can be contract, using Lemma 28 with $x=p^{\tau-1}-2p^{\tau-2}-\sum_{i=0}^{\tau-3}p^i-1$, $y=\sum_{i=0}^{\tau-1}p^i+1$ and $z=p-2$, to $2p^{\tau-1}-p^{\tau-2}$ variables of type C^2. With Lemma 40, those and the $2p-2$ variables in E_ν^j for $j\in\{2,\dots,\tau-1\}$ can be contracted to a $C^{\tau+1}$ variable. Thus, from now on, one can assume that

$$I_{\max}^1\leq p^\tau+4p^{\tau-1}-\frac{p-1}{2}\sum_{i=1}^{\tau-2}p^i+3\sum_{i=0}^{\tau-3}p^i-p-5. \tag{2.7.5}$$

If $q_1\geq p^\tau+p-2=\left(\sum_{i=0}^{\tau-1}p^i+1\right)(p-1)$ and $m_1\geq 2p^\tau+p^2-p-3=\left(\sum_{i=0}^{\tau-1}p^i+1\right)(2p-2)+p^2-3p+1$, one can use Lemma 36 to contract the E_0^0 variables to $2p-2$ variables of type E_0^i for all $i\in\{0,\dots,\tau-1\}$ because $I_0^0\geq p^{\tau+1}+p^\tau-1\geq 4p^\tau-\frac{p-1}{2}\sum_{i=1}^{\tau-1}p^i+3\sum_{i=0}^{\tau-2}p^i-2p-2$. By Lemma 33, the $p^{\tau+1}-p^\tau$ variables of type C^0 can be contracted together with the $2p-2$ variables of type E_0^0 to $p^\tau-p^{\tau-1}$ variables of type C^1. Using Lemma 30 with $x=p^{\tau-1}-2p^{\tau-2}-\sum_{i=0}^{\tau-3}p^i-1$, $y=\sum_{i=0}^{\tau-1}p^i+1$ and $z=p-2$, one can contract the E^1 variables together with the C^1 variables to $2p^{\tau-1}-p^{\tau-2}$ variables of type C^2, which contract together with the $2p-2$ variables of type E_0^i for $i\in\{2,\dots,\tau-1\}$ to a $C^{\tau+1}$ variables due to Lemma 40. Therefore, one can assume that either $m_1\leq 2p^\tau+p^2-p-4$ or $q_1\leq p^\tau+p-3$. The latter case leads to $m_1=q_1+I_{\max}^1\leq 2p^\tau+4p^{\tau-1}-\frac{p-1}{2}\sum_{i=1}^{\tau-2}p^i+3\sum_{i=0}^{\tau-3}p^i-8$ due to (2.7.5). Hence, from now on, one can assume that

$$m_1\leq 2p^\tau+4p^{\tau-1}-\frac{p-1}{2}\sum_{i=1}^{\tau-2}p^i+3\sum_{i=0}^{\tau-3}p^i+p^2-8, \tag{2.7.6}$$

because this is an upper bound for the upper bound for m_1 in both cases.

By the p-normalisation of f,g, it follows that

$$I_0^0\geq 4p^{\tau+1}-4p^\tau+1-q_0-m_1\geq 3p^{\tau+1}-6p^\tau-4p^{\tau-1}-3\sum_{i=0}^{\tau-3}p^i-p^2+10. \tag{2.7.7}$$

Therefore, one has $I_{00}^0\geq 3p^\tau-6p^{\tau-1}-4p^{\tau-2}-3\sum_{i=0}^{\tau-4}p^i-p\geq p^{\tau-1}+2p-3$ and, due to (2.4.1), it follows that

$$\begin{aligned}I_0^0-I_{00}^0&\geq 2p^{\tau+1}-2p^\tau-q_0-\left(m_1-I_0^1\right)\geq p^{\tau+1}-2p^\tau+1-\left(m_1-I_0^1\right)\\&\geq p^{\tau-1}+2p-3-\left(m_1-I_0^1\right).\end{aligned}$$

It follows from (2.7.7) that $I_0^0\geq p^\tau+2p^2-3p-p\left(m_1-I_0^1\right)+p^2-3p+3$, and thus, if $m_1-I_0^1\leq p^{\tau-1}+2p-3$, one can contract $p^\tau+2p^2-3p-p\left(m_1-I_0^1\right)$ of the E_0^0 variables to $p^{\tau-1}+2p-3-\left(m_1-I_0^1\right)$ variables of type $E_{\bar{0}}^1$ with Lemma 31. There are at least $3p^{\tau+1}-7p^\tau-4p^{\tau-1}-3\sum_{i=0}^{\tau-3}p^i-3p^2+3p+10$

variables of type E_0^0 remaining, which contract to

$$\left\lceil \frac{3p^{\tau+1} - 7p^\tau - 4p^{\tau-1} - 3\sum_{i=0}^{\tau-3} p^i - 3p^2 + 3p + 10}{p} \right\rceil - 2p + \frac{p-3}{2}$$
$$\geq 3p^\tau - 7p^{\tau-1} - 4p^{\tau-2} - 3\sum_{i=0}^{\tau-4} p^i - 5p + \frac{p-3}{2} + 4$$

variables of type E_0^1 with Lemma 27, while leaving at least $6p-9 \geq 2p-2$ variables of type E_0^0 unused. This is at least as big as $p^{\tau-1} + 2p - 3$. Thus, one has at least $p^{\tau-1} + 2p - 3$ variables of type E_0^1, as well as a total of $p^{\tau-1} + 2p - 3$ variables of type $E_{\bar{0}}^1$. By Lemma 33, one can contract $p^{\tau+1} - p^\tau$ of the C^0 variables with the remaining $2p-2$ variables of type E_0^0 to $p^\tau - p^{\tau-1}$ variables of type C^1 and then use Lemma 28 with $x = p^{\tau-1} - \sum_{i=0}^{\tau-2} p^i - 1$, $y = \sum_{i=0}^{\tau-2} p^i + 2$ and $z = p-3$ to contract them together with the E^1 variables to $p^{\tau-1}$ variables of type C^2.

For $\tau = 2$ it follows for $p \geq 7$, due to (2.7.3) and (2.7.6), that

$$m_2 \geq 3p^3 - \frac{33}{2}p^2 + \frac{5}{2}p + 10 \geq p^2 - p - 1 = (p-2)(p+1) + 1,$$

and for $p = 5$, due to (2.7.4) and (2.7.6), that

$$m_2 \geq 2p^3 - 10p^2 + 3p + 10 \geq p^2 - p - 1 = (p-2)(p+1) + 1.$$

Therefore, one has a μ with $I_\mu^2 \geq p-1$, from which it follows that one can contract the p variables of type C^2 and the $p-1$ variables of type E_μ^2 to a $C^3 = C^{\tau+1}$ variable due to Lemma 22. Thus, from now on, one can assume that $\tau \geq 3$.

If $I_\mu^2 = I_{\max}^2 \geq 2p^{\tau-1} + 4p^{\tau-2} - \frac{p-1}{2}\sum_{i=1}^{\tau-3} p^i - p^{\tau-3} + 3\sum_{i=0}^{\tau-4} p^i - 2p - 2$, one can use Lemma 34 to contract the E_μ^2 variables to $p-1$ variables of type E_μ^τ and $2p-2$ variables of type E_μ^i for all $i \in \{2, \dots, \tau-1\}$. It follows that one can contract them together with the C^2 variables to a $C^{\tau+1}$ variable due to Lemma 40. From now on, one can assume that

$$I_{\max}^2 \leq 2p^{\tau-1} + 4p^{\tau-2} - \frac{p-1}{2}\sum_{i=1}^{\tau-3} p^i - p^{\tau-3} + 3\sum_{i=0}^{\tau-4} p^i - 2p - 3,$$

and, therefore,

$$m_2 \leq 2p^\tau + 6p^{\tau-1} + 3p^{\tau-2} + 2p^{\tau-3} + 6\sum_{i=0}^{\tau-4} p^i - 2p^2 - 5p - 3. \tag{2.7.8}$$

Then one can contract the $p^{\tau-1}$ variables of type C^2 to $p^{\tau-2} - 2$ variables of type C^3 using Lemma 32. Due to (2.7.3), (2.7.6) and (2.7.8), it follows that

$$m_0 + m_1 + m_2 \leq 3p^{\tau+1} + \frac{19}{2}p^\tau + \frac{17}{2}p^{\tau-1} + 6p^{\tau-2} + 8p^{\tau-3} + 12\sum_{i=0}^{\tau-4} p^i + p^2 - 10p - 15,$$

which does not only hold for $p \geq 7$ but also for $p = 5$ because the upper bound (2.7.3) is in the

case $p = 5$ bigger than the upper bound (2.7.4). This leads to

$$q_3 \geq 4p^{\tau+1} - \frac{33}{2}p^{\tau} - \frac{17}{2}p^{\tau-1} - 6p^{\tau-2} - 8p^{\tau-3} - 12\sum_{i=0}^{\tau-4} p^i - p^2 + 10p + 16 \geq p^{\tau-2} + p^{\tau-3} - 2$$

and

$$\begin{aligned} m_3 &\geq 5p^{\tau+1} - \frac{35}{2}p^{\tau} - \frac{17}{2}p^{\tau-1} - 6p^{\tau-2} - 8p^{\tau-3} - 12\sum_{i=0}^{\tau-4} p^i - p^2 + 10p + 16 \\ &\geq 2p^{\tau-2} + 2p^{\tau-3} + p^2 - 3p - 3. \end{aligned}$$

For $\tau = 3$ one can contract one of the C^3 variables together with the E^3 variables to a C^4 variable using Lemma 29 with $x = 1$. For $\tau \geq 4$ the C^3 variables can be contracted with the E^3 variables, using Lemma 30 with $x = p^{\tau-3} - p^{\tau-4} - 2\sum_{i=0}^{\tau-5} p^i - 1$, $y = p^{\tau-3} + 2\sum_{i=0}^{\tau-4} p^i$ and $z = p - 4$, to $2p^{\tau-3} + p^{\tau-4} - 1$ variables of type C^4. Then one can use first Lemma 32 to contract them to $2p - 1$ variables of type C^{τ} and then Lemma 15 to contract them to a $C^{\tau+1}$ variable. □

Lemma 47. *Let f, g be a proper p-normalised pair with $\tau \geq 2$, $r = r(f,g) = -1$ and $I_0^0 \leq p^{\tau+1} + p^{\tau} - 2$. Then the equations $f = g = 0$ have a non-trivial p-adic solution.*

Proof. Due to the upper bound for I_0^0 and $r = -1$ it follows that

$$m_0 \leq p^{\tau+1} + p^{\tau} - 2 + p^{\tau+1} - 1 = 2p^{\tau+1} + p^{\tau} - 3 \tag{2.7.9}$$

and, hence,

$$q_1 \geq 3p^{\tau+1} - 3p^{\tau} + 1 - 2p^{\tau+1} - p^{\tau} + 3 = p^{\tau+1} - 4p^{\tau} + 4 \geq p^{\tau} + p - 2 \tag{2.7.10}$$

and

$$m_1 \geq 4p^{\tau+1} - 4p^{\tau} + 1 - 2p^{\tau+1} - p^{\tau} + 3 = 2p^{\tau+1} - 5p^{\tau} + 4 \geq 2p^{\tau} + p^2 - p - 3. \tag{2.7.11}$$

Use Lemma 24 to contract the E^0 variables to $p^{\tau} - p^{\tau-1}$ variables of type P^1.

If $I_{\nu}^1 = I_{\max}^1 \geq p^{\tau} + 4p^{\tau-1} - \frac{p-1}{2}\sum_{j=1}^{\tau-2} p^j + 3\sum_{j=0}^{\tau-3} p^j - p - 4$, one can contract $4p^{\tau-1} - \frac{p-1}{2}\sum_{i=1}^{\tau-2} p^i + 3\sum_{i=0}^{\tau-3} p^i - 2p - 2$ of the variables of type E_{ν}^1 to $2p-2$ variables of type E_{ν}^j for all $j \in \{1, \ldots, \tau-1\}$ using Lemma 36, which leaves $p^{\tau} + p - 2$ variables of type E_{ν}^1 unused. Then Lemma 28 can be used with $x = p^{\tau-1} - 2p^{\tau-2} - \sum_{i=0}^{\tau-3} p^i - 1$, $y = \sum_{i=0}^{\tau-1} p^i + 1$ and $z = p - 2$ to contract the remaining E_{ν}^1 variables together with the $p^{\tau} + p - 2$ variables of type $E_{\bar{\nu}}^1$ and the P^1 variables to $2p^{\tau-1} - p^{\tau-2}$ variables of type P^2. Those and the $2p - 2$ variables in E_{ν}^j for $j \in \{2, \ldots, \tau-1\}$ can be contracted to a $P^{\tau+1}$ variable, using Lemma 40.

Thus, one can furthermore assume that one has $I_{\nu}^1 = I_{\max}^1 \leq p^{\tau} + 4p^{\tau-1} - \frac{p-1}{2}\sum_{i=1}^{\tau-2} p^i + 3\sum_{i=0}^{\tau-3} p^i - p - 5$. It follows that

$$m_1 \leq p^{\tau+1} + 5p^{\tau} + 4p^{\tau-1} + 3p^{\tau-2} + 6\sum_{i=0}^{\tau-3} p^i. \tag{2.7.12}$$

Due to (2.7.10) and (2.7.11), one can use Lemma 30 with $x = p^{\tau-1} - 2p^{\tau-2} - \sum_{i=0}^{\tau-3} p^i - 1$, $y = \sum_{i=0}^{\tau-1} p^i + 1$ and $z = p - 2$ to contract the $p^{\tau} - p^{\tau-1}$ variables of type P^1 and the E^1 variables to $2p^{\tau-1} - p^{\tau-2}$ variables of type P^2. For $\tau = 2$, one can use Lemma 15 to contract the $2p - 1$

variables of type P^2 to a $P^3 = P^{\tau+1}$ variable. Hence, one can assume that $\tau \geq 3$. As a consequence of (2.7.9) and (2.7.12), it follows that

$$\begin{aligned} m_2 &\geq 6p^{\tau+1} - 6p^{\tau} + 1 - 2p^{\tau+1} - p^{\tau} + 3 - p^{\tau+1} - 5p^{\tau} - 4p^{\tau-1} - 3p^{\tau-2} - 6\sum_{i=0}^{\tau-3} p^i \\ &= 3p^{\tau+1} - 12p^{\tau} - 4p^{\tau-1} - 3p^{\tau-2} - 6\sum_{i=0}^{\tau-3} p^i + 4, \end{aligned}$$

which is bigger than $(p+1)\left(4p^{\tau-2} - \frac{p-1}{2}\sum_{i=1}^{\tau-3} p^i + 3\sum_{i=0}^{\tau-4} p^i - 2p - 2\right)$. Hence, there is a μ such that $I_\mu^2 \geq 4p^{\tau-2} - \frac{p-1}{2}\sum_{i=1}^{\tau-3} p^i + 3\sum_{i=0}^{\tau-4} p^i - 2p - 2$, thus, one can contract the E_μ^2 variables using Lemma 36 and then the resulting variables together with the P^2 variables to a $P^{\tau+1}$ variable, using Lemma 40. □

It follows that for a proper p-normalised pair f, g with $\tau \geq 2$ the equations $f = g = 0$ have a non-trivial p-adic solution, which in combination with Section 2.6 proves the claim of Theorem 1.

3 Beyond Artin's Conjecture for Cubic Forms

This chapter comprises the authors article *Beyond Artin's Conjecture for Cubic Forms* [24]. It contains the proof of the following theorem, which claims that for one diagonal cubic form f and one linear form g in s variables the equations $f = g = 0$ have a non-trivial p-adic solution for all primes p provided that $s \geq 8$.

Theorem 2. *Let $s \geq 8$ and $a_i, b_i \in \mathbb{Z}$ for $1 \leq i \leq s$. Then the system*

$$\sum_{j=1}^{s} a_j x_j^3 = \sum_{j=1}^{s} b_j x_j = 0, \tag{1.0.4}$$

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

This is an improvement upon the authors master thesis, where the corresponding statement for $s \geq 9$ was proved. The proof given in Section 3.1 for the case $p \equiv 2 \bmod 3$ is the same as the one given in the master thesis for $s \geq 9$ as it holds in the stronger case $s \geq 8$ as well. Furthermore, Lemmata 54 to 63 and 87 to 98 as well as Conclusions 2 to 9 and their proofs are adopted directly from the master thesis. Even though the statements of the lemmata in the master thesis corresponding to Lemmata 57 and 58 are weaker, the proofs hold for this stronger version as well.

3.1 The Case $p \equiv 2 \bmod 3$

This section contains the proof of Theorem 2 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

$$c_1 x_1^3 + \ldots + c_t x_t^3 = 0, \tag{3.1.1}$$

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 [17] denoted the smallest t such that a non-trivial p-adic solution exists for all equations (3.1.1) by $\Gamma^*(3, p)$. More general, $\Gamma^*(k, p)$ denotes the smallest number $t \in \mathbb{N}$, such that for all $c_1, \ldots, c_t \in \mathbb{Z}$ the equation

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

has a solution $\mathbf{x} \in \mathbb{Q}_p^t \backslash \{\mathbf{0}\}$. Brüdern and Robert [9, Section 3] transformed a system (1.0.4) into an equation of the shape (3.1.1) to prove that, provided that $\Gamma^*(3, p)$ is small in relation to s, a system (1.0.4) has a non-trivial p-adic solution.

Lemma 48. *Suppose $s \geq 2\Gamma^*(k,p)$. Then the system*

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

has a non-trivial solution in $\mathbb{Q}_p$.

Proof. See [9, Lemma 3.1]. □

All that remains to be shown is that $\Gamma^*(3,p) \leq 4$ for all p congruent to 2 modulo 3. Dodson [17] defined $\gamma^*(k,p^n)$ as the least positive integer t with the property that if $c_1,\ldots,c_t$ are any integers coprime to p, then the congruence

$$c_1 x_1^k + \ldots + c_t x_t^k \equiv 0 \mod p^n$$

has a primitive solution, that is an integer solution with not all variables $x_1,\ldots,x_t$ 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 $\left\{x^k \mid x \in \mathbb{F}_p\right\}$ and $\left\{x^\delta \mid x \in \mathbb{F}_p\right\}$ 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 49. *It holds* $\Gamma^*(k,p) \leq k(\gamma^*(k,p^\gamma)-1)+1.$

Proof. See [17, Lemma 4.2.1]. □

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

$$\Gamma^*(3,p) \leq 3\,(\gamma^*(3,p)-1)+1.$$

Here, one has $\gamma^*(3,p) = \gamma^*(1,p)$, which is obviously 2 and hence $\Gamma^*(3,p) \leq 4$. The only remaining prime $p \equiv 2 \bmod 3$ is 2. Lemma 49 can be applied to show that

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

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

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

Hence, it holds $\Gamma^*(3,2) \leq 4$ as well and Theorem 2 is fulfilled for all primes p congruent to 2 modulo 3.

For primes congruent to 1 modulo 3 this does not give the desired result because $\Gamma^*(k,p)$ is too large. For them, a special case of Hensel's lemma by Brüdern and Robert [9, Lemmata 4.1 and 4.2] can be used to reduce the problem to one of congruences.

3.2 A Special Case of Hensel's Lemma

Throughout this section 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 (1.0.4) are used. In Theorem 2, this degree is 3 and, hence, one has $\gamma = \tau + 1$, where $\tau = 0$ for all $p > 3$ and $\tau = 1$ for $p = 3$. The following lemma was proved by Brüdern and Robert [9, Lemma 4.2]. Although they excluded $k = 3$ before they proved it, the proof for $k = 3$ and $p > 2$ is the same.

Lemma 50. *Let $s \geq 2$, $p > 2$ be a prime, γ defined as in the previous section and suppose that $\mathbf{x} \in \mathbb{Z}^s$ satisfies the congruences*

$$\sum_{j=1}^{s} a_j x_j^3 \equiv 0 \mod p^\gamma, \quad \sum_{j=1}^{s} b_j x_j \equiv 0 \mod p \tag{3.2.1}$$

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

$$a_1 y_1^3 + a_2 y_2^3 + \sum_{j=3}^{s} a_j x_j^3 = b_1 y_1 + b_2 y_2 + \sum_{j=3}^{s} b_j x_j = 0.$$

For the remainder of this chapter a simultaneous solution of

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

is called *non-singular* if there are $1 \leq i, j \leq s$ 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 summarised to the following result.

Lemma 51. *Let $s \geq 2$, $p > 2$ prime, γ defined as in the previous section and suppose that the equations*

$$\sum_{j=1}^{s} a_j x_j^3 \equiv 0 \mod p^\gamma, \quad \sum_{j=1}^{s} b_j x_j \equiv 0 \mod p \tag{3.2.2}$$

have a non-singular solution. Then (1.0.4) has a non-trivial p-adic one.

3.3 Conditioned Systems

This section contains a description of conditioned systems, introduced by Brüdern and Robert [9], which are a variant of the p-normalised systems by Davenport and Lewis [12]. One says that two systems (1.0.4) 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.

It can be easily seen that if one representative of an equivalence class has a non-trivial p-adic solution, so has the whole class.

Brüdern and Robert [9, Section 6] showed that every system (1.0.4) with $a_i, b_i \in \mathbb{Q}\backslash\{0\}$ for $1 \le i \le s$ 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 $1 \le j \le 3$.

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

Lemma 52. *Suppose that for a fixed s there is a non-trivial p-adic solution for all conditioned systems. Then all systems* (1.0.4) *with rational coefficients have non-trivial p-adic solutions.*

Proof. See [9, Lemma 6.1]. □

The work with conditioned systems and systems (1.0.4) requires the following notation.

(i) For $1 \le i \le s$, 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 $1 \le i \le s$ with $\nu_i = \mu_i = 0$.

(iii) For $j \in \mathbb{N}_0$, the parameter v_j is defined as the number of $1 \le i \le s$ 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 with $s \ge 8$ that $\nu_i \in \{0, 1, 2\}$, $v_0 \ge 3$, $v_0 + v_1 \ge 6$ and $v_0 + v_1 + v_2 = s$.

The set of systems

$$\sum_{j=1}^{s} a_j x_j^3 = \sum_{j=1}^{s} b_j x_j = 0 \tag{3.3.1}$$

with non-zero integers coefficients where $p^3 \nmid a_i$ $(1 \le i \le s)$ includes the set of conditioned systems. For each system (3.3.1) one can find integers $\alpha_i \in \mathbb{Z}$ such that $\alpha_i p^{-\mu_i} b_i \equiv 1 \bmod p$ for all $1 \le i \le s$, because $p^{\mu_i} \| b_i$. Applying $x_i \mapsto \alpha_i x_i$ for $1 \le i \le n$ provides an equivalent system with $p^{-\mu_i} b_i \equiv 1 \bmod p$. As this transformation does not modify the parameters v_i and t, one can assume that every system (3.3.1) and, hence, every conditioned system has this property.

In the following, all conditioned systems are divided into different sets, depending on the parameter used to describe them, to prove that they all have a non-trivial solution p-adic solution. To make the proofs 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 permuting 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 $(0 \le i \le 2)$ 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 10. A system (3.3.1) is called an *ordered system* (3.3.1) 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 (3.3.1) is also conditioned, it is called an *ordered conditioned system.*

As every system (1.0.4) 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 lemmata are slightly more general than others, which proves to be useful.

3.4 The Case $p \equiv 1 \bmod 3$

As shown in Section 3.2, one has to handle congruences modulo p, for which the following lemmata are useful tools.

Lemma 53. *Let p be a prime, $\delta = (k, p-1)$, $p > 2\delta + 1$ and $\alpha_1 \ldots \alpha_n \not\equiv 0 \bmod p$. Then*

$$\alpha_1 x_1^k + \ldots + \alpha_n x_n^k \tag{3.4.1}$$

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

Proof. See [10]. □

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 a prime 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

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

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 54. *Let $\alpha_1\alpha_2\alpha_3 \not\equiv 0 \bmod 7$. Then*

$$\alpha_1 x_1^3 + \alpha_2 x_2^3 + \alpha_3 x_3^3 \equiv 0 \mod 7 \tag{3.4.2}$$

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 (3.4.2) into 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 shape

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

Setting $x_1 = x_2 = -x_3 = 1$, one obtains a non-trivial solution. Else there are $1 \le i < j \le 3$ 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 zero. □

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

Lemma 55. *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 54 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 first three 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 (3.3.1).

Lemma 56. *Let $p \equiv 1 \bmod 3$ be a prime. An ordered system* (3.3.1) *with $v_0 \geq 3$ and a low variable at level* 0 *has a non-trivial p-adic solution.*

Proof. The variables $x_1, \ldots, x_{v_0}$ 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

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

for which Lemma 55 provides a non-singular solution. Hence, Lemma 51 can be used to lift the non-singular solution to a non-trivial p-adic one. □

Lemma 57. *Let $p \equiv 1 \bmod 3$ be a prime. Suppose $v_j \geq 3$ for $j \in \{1, 2\}$. Then an ordered conditioned system has a non-trivial p-adic solution if $s \geq 8$.*

Proof. An ordered conditioned system with $s \geq 8$ has by definition $v_0 \geq 3$ and, hence, if it has a low variable at level 0, the existence of a non-trivial p-adic solution follows from Lemma 56.

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

$$\sum_{i=1}^{s} a_i x_i^3 = f_0(\mathbf{x}_0) + p f_1(\mathbf{x}_1) + p^2 f_2(\mathbf{x}_2), \tag{3.4.3}$$

where $f_j(\mathbf{x}_j) = p^{-j} \sum_{\nu_i = j} a_i x_i^3$ are polynomials in $\mathbb{Z}[x_1, \ldots, x_s]$. Apply $x_i \mapsto p x_i$ for $1 \leq i \leq v_0$ or $1 \leq i \leq v_0 + v_1$ 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 (3.3.1) and changes (3.4.3) 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 $p \mid a_1$ and $p \nmid b_1$, hence, $v_0 \geq 3$ and it exists a low variable at level 0. By applying a permutation of indices one obtains an ordered system (3.3.1), hence, all conditions of Lemma 56 are fulfilled and a non-trivial p-adic solution exists. □

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

Lemma 58. *If an ordered conditioned system with $s \geq 8$ does not have a non-trivial p-adic solution for all primes p congruent to 1 modulo 3, then*

$$v_0 \geq 4, \qquad v_1 \leq 2, \qquad v_2 \leq 2$$

and there is no low variable at level 0.

Proof. It follows from Lemma 57 that v_1 and v_2 have to be at most 2. But since $s \geq 8$ one obtains the lower bound $v_0 \geq 4$. Furthermore, Lemma 56 can be applied to show that no low variable at level 0 exist. □

To prove Theorem 2 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 (3.3.1) described in Lemma 58, which can be divided up into different sets, depending on the correlation between v_0 and t.

Lemma 59. *Let $p \equiv 1 \bmod 3$ be a prime. An ordered conditioned system with $v_0 \geq t+3$ has a non-trivial p-adic solution.*

Proof. Set $x_i = 0$ for all $1 \leq i \leq t$ and $t+4 \leq i \leq s$. 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 for $p > 7$ and Lemma 54 for $p = 7$ provide a non-trivial solution of the cubic equation

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

with $x_{t+j} \not\equiv 0 \bmod p$ 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 51. □

Lemma 60. *Let $p \equiv 1 \bmod 3$ be a prime. Let $3 \leq m \leq n$ and $a_i \not\equiv 0 \bmod p$ for $1 \leq i \leq n$. If there are $1 \leq i < j \leq m$ such that $a_i \equiv a_j \bmod p$, then the equations*

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

have a non-singular solution.

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

$$\begin{aligned} a_1x_1^3 + \ldots + a_mx_m^3 + a_{m+1}x_{m+1}^3 + \ldots + a_nx_n^3 &\equiv a_ix_i^3 + a_jx_j^3 \equiv a_i - a_j \equiv 0 \mod p, \\ x_1 + \ldots + x_m &\equiv x_i + x_j \equiv 1 - 1 \equiv 0 \mod p, \end{aligned}$$

and there is a $k \neq i,j$ with $1 \leq k \leq m$, 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 $v_0 = t+2 \geq 5$ and $v_0 = t+1 \geq 5$, as is done in the next two lemmata.

Lemma 61. *Let $p \equiv 1 \bmod 3$ be a prime. An ordered conditioned system with $v_0 = t + 2 \geq 5$ has a non-trivial p-adic solution.*

Proof. If $a_1 \equiv a_2 \bmod p$, Lemma 60 provides a non-singular solution as $t \geq 3$. If they are distinct modulo p, setting all variables zero, except x_1, x_2, x_{t+1} and x_{t+2}, transforms the system into

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

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

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

Conclusion 1 for $p > 7$ and Lemma 54 for $p = 7$ 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 $a_i x_i^2 b_3 - b_i a_3 x_3^2 \equiv b_3 a_i x_i^2 \not\equiv 0 \bmod p$ this is a non-singular solution and Lemma 51 provides the required non-trivial p-adic solution. □

Lemma 62. *Let $p \equiv 1 \bmod 3$ be a prime. An ordered conditioned system with $v_0 = t + 1 \geq 5$ has a non-trivial p-adic solution.*

Proof. Set all variables zero except $x_1, \ldots, x_4$ and x_{v_0}. The obtained system has the shape

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

If two of the coefficients $a_1, \ldots, a_4$ are equivalent modulo p, Lemma 60 provides a non-singular solution. Else, one can assume that all a_i modulo p are distinct for $1 \leq i \leq 4$. Set $x_1 = -x_2 = y_1$ and $x_3 = -x_4 = y_2$. It follows that

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

As both $a_1 - a_2$ and $a_3 - a_4$ are not congruent to 0 modulo p, Conclusion 1 for $p > 7$ and Lemma 54 for $p = 7$ 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 51 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 disjoint union of $(\mathbb{F}_p^*)^3$ and its two cosets. Every element in one of the three cosets can be transformed in any other element in the same coset by multiplying it with a cube.

Lemma 63. *Let $p \equiv 1 \bmod 3$ be a prime. An ordered conditioned system with $t \geq 5$ has a non-trivial p-adic solution.*

Proof. If $a_1, \ldots, a_5$ are not distinct modulo p, Lemma 60 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 $(\mathbb{F}_p^*)^3$. 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 $b^3 a_1 \equiv a_2 \bmod p$. Put $x_1 = by$, $x_2 = -y$ and $x_i = 0$ for all $i \geq 6$. This transforms the cubic equation of the system into

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

and the linear equation into

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

Conclusion 1 for $p > 7$ and Lemma 54 for $p = 7$ provide a non-trivial solution of the cubic equation with an $i \in \{3, 4, 5\}$ such that $x_i \not\equiv 0 \bmod p$. As $b - 1 \not\equiv 0 \bmod p$ 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 $y \equiv 0 \bmod p$. If $y \not\equiv 0 \bmod p$ then $b_2a_1x_1^2 - b_1a_2x_2^2 \equiv a_1b^2y^2 - a_1b^3y^2 \equiv a_1b^2y^2\,(1-b) \not\equiv 0 \bmod p$, else, $y \equiv 0 \bmod p$ and $b_1a_ix_i^2 - b_ia_1x_1^2 \equiv a_ix_i^2 - a_1b^2y^2 \equiv a_ix_i^2 \not\equiv 0 \bmod p$. This proves that there is a non-singular solution, which can be lifted to a non-trivial p-adic one by Lemma 51. □

The cases not yet proved are those with $(v_0, t) \in \{(4,2), (4,3), (4,4)\}$. These more complex cases are treated in the following two sections.

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

Proof. Setting $x_1 = 1$, $x_2 = -1$ and $x_i = 0$ for $i \geq 5$ solves the linear equation. The cubic equation transforms into $a_1 - a_2 + a_3x_3^3 + a_4x_4^3 \equiv 0 \bmod p$, which has, due to Conclusion 1, a solution which is non-singular as $a_1x_1^2b_2 - a_2x_2^2b_1 \equiv a_1 - a_2 \not\equiv 0 \bmod p$ and can be lifted with Lemma 51. □

Lemma 65. *An ordered conditioned system with $v_0 = 4$ and $t = 2$, where $a_1 \not\equiv a_2 \bmod 7$, has a non-trivial 7-adic solution.*

Proof. A multiplication of the cubic equation with α such that $\alpha a_3 \equiv 1 \bmod 7$ still leaves $a_1 \not\equiv a_2 \bmod 7$. 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 $a_4 \equiv 1 \bmod 7$, set $x_3 = 1$, $x_4 = -1$ and everything else zero. This solves the cubic and the linear equation modulo 7 and because $a_3x_3^2b_1 - a_1x_1^2b_3 \equiv a_3 \equiv 1 \bmod 7$ this solution is non-singular. The cases with $a_4 \equiv 2, 3 \bmod 7$ can be solved by choosing $x_3, x_4 \in \{-1, 0, 1\}$, not both 0, such that $a_3x_3^3 + a_4x_4^3 \equiv \pm(a_1 - a_2) \bmod 7$ and then setting

$x_1 = \mp 1$ and $x_2 = \pm 1$, such that the cubic solution is solved as well as the linear one modulo 7. Let $i \in \{3, 4\}$ be such that $x_i \not\equiv 0 \bmod 7$. Then $a_i x_i^2 b_1 - a_1 x_1^2 b_i \equiv a_i \not\equiv 0 \bmod 7$. Both times the solution can be lifted with Lemma 51. □

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

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

Definition 11. 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 66. *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 $a_{2i+3} \equiv c^3 a_{2i+4} \bmod p$ for some $c \not\equiv 0 \bmod p$. Set all variables zero 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 $\nu_1 = 3 - i \geq 1$, $\nu_{2i+3} = \nu_{2i+4} = 0$, $\mu_1 = 0$ and $\mu_{2i+3}, \mu_{2i+4} \geq 0$. 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 51. □

Definition 12. 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 $a_1 - a_2 = p^\theta a'$ and $p \nmid a'$ 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 $t = 2$, one has to prove that every critical system has a non-trivial p-adic solution for all primes $p \equiv 1 \bmod 3$. For that, the following lemmata are useful, first among them one, similar to Lemma 54, fitting better for critical systems which is proceeded by a tool which uses the knowledge about a_1 and a_2.

Lemma 67. *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, one 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 zero. Else, one has $c_i \in \{\pm 2, \pm 3\}$, 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 68. *Let $p \equiv 1 \bmod 3$ be a prime, $a_1 - a_2 = p^\theta a'$ for some $\theta \in \mathbb{N}$ with $p \nmid a'$ and $a_1 \equiv a_2 \equiv 1 \bmod p$. Let c and d be integers with $p \nmid cd$ and $\left(\frac{cd}{p}\right) = \left(\frac{3}{p}\right)$, where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. Then, for each l with $1 \leq l < \theta$, 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 $3a_1 x^2 d \equiv c \bmod p$. 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

$$\begin{aligned} a_1 x_1^3 + a_2 x_2^3 &= a_1 x^3 + 3a_1 x^2 d p^l + 3a_1 x d^2 p^{2l} + a_1 d^3 p^{3l} - a_2 x^3 \\ &= p^\theta a' x^3 + 3a_1 x^2 d p^l + 3a_1 x d^2 p^{2l} + a_1 d^3 p^{3l} \\ &\equiv 3a_1 x^2 d p^l \equiv c p^l \mod p^{l+1}, \end{aligned}$$

and, hence, $a_1 x_1^3 + a_2 x_2^3 = c' p^l$ for some $c' \equiv c \bmod p$. □

Lemma 69. *Let $p \equiv 1 \bmod 3$ be a prime, $a_1 - a_2 = p^\theta a'$ for some $\theta \in \mathbb{N}$ with $p \nmid a'$, $a_1 \equiv a_2 \equiv 1 \bmod p$, $c_1, c_2, d_1, d_2, e, f \in \mathbb{Z}$ such that $p \nmid c_1 c_2 f$, $[c_1] \neq [c_2]$ and $1 \leq \beta < \theta$. Then the system of equation*

$$\begin{aligned} a_1 x_1^3 + a_2 x_2^3 + p^\beta \left(c_1 y_1^3 + c_2 y_2^3\right) + p^{\beta+1} e z^3 &= 0, \\ x_1 + x_2 + p^\beta \left(d_1 y_1 + d_2 y_2\right) + p^\beta f z &= 0 \end{aligned}$$

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 68 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

$$a_1 x_1^3 + a_2 x_2^3 + p^\beta \left(c_1 y_1^3 + c_2 y_2^3\right) + p^{\beta+1} e z^3 = p^\beta c' + p^\beta \left(c_1 y_1^3 + c_2 y_2^3\right) + p^{\beta+1} e z^3$$

and

$$x_1 + x_2 + p^\beta \left(d_1 y_1 + d_2 y_2\right) + p^\beta f z = p^\beta d + p^\beta \left(d_1 y_1 + d_2 y_2\right) + p^\beta f z.$$

Dividing both equation by p^β leaves the system

$$\begin{aligned} c' + c_1 y_1^3 + c_2 y_2^3 + p e z^3 &= 0, \\ d + d_1 y_1 + d_2 y_2 + f z &= 0 \end{aligned}$$

to be solved. Setting $y_1 = y_2 = 1$, the upper equation is solved modulo p and choosing z such that the lower equation is solved modulo p gives a solution of the system modulo p. Since

$c_1 y_1^2 f - pez^2 d_1 \equiv c_1 f \not\equiv 0 \bmod p$ this solution can be lifted with Lemma 51 to a solution in $\mathbb{Q}_p^5$ of the system. □

Lemma 70. *A critical system with a low variable at level $\beta < \theta$ has a non-trivial p-adic solution for primes $p \equiv 1 \bmod 3$.*

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, $1 \le \beta \le \theta - 1$. 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 zero, except x_1, x_2, $x_{2\beta+3}$, $x_{2\beta+4}$ and x_t. This is a system as in Lemma 69, hence, it has a non-trivial p-adic solution. □

Lemma 71. *Let $p \equiv 1 \bmod 3$ be a prime, $a_1 - a_2 = p^\theta a'$ for some $\theta \in \mathbb{N}$ with $p \nmid a'$, $a_1 \equiv a_2 \equiv 1 \bmod p$, $c_1, c_2, d_1, d_2 \in \mathbb{Z}$ such that $p \nmid c_1 c_2 d_1$, $d_1 \equiv 1 \bmod p$ and d_2 is congruent to either 0 or 1 modulo p. Let furthermore $c_1 \not\equiv c_2 \bmod p$ and $1 \le \beta \le \theta - 3$. Then the system of equations*

$$\begin{aligned} a_1 x_1^3 + a_2 x_2^3 + p^\beta \left(c_1 y_1^3 + c_2 y_2^3\right) &= 0, \\ x_1 + \quad x_2 + p^\beta \left(d_1 y_1 + d_2 y_2\right) &= 0 \end{aligned}$$

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

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

where the upper equation can be divides by $p^{\beta+3}$ and the lower one by $p^{\beta+1}$.

In the case $d_2 \equiv 0 \bmod p$, this transforms the system modulo p into

$$\begin{aligned} a' p^{\theta-\beta-3} + 3d + c_1 y_1'^3 + c_2 y_2'^3 &\equiv 0 \mod p, \\ y_1' &\equiv 0 \mod p. \end{aligned}$$

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, due to $c_1 y_1'^2 d_2 - c_2 y_2'^2 d_1 \equiv -c_2 \not\equiv 0 \bmod p$.

In the case $d_2 \equiv 1 \bmod p$, this transforms the system modulo p into

$$\begin{aligned} a' p^{\theta-\beta-3} + 3d + c_1 y_1'^3 + c_2 y_2'^3 &\equiv 0 \mod p, \\ y_1' + y_2' &\equiv 0 \mod p. \end{aligned}$$

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 51. □

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

Lemma 72. *An absolutely irreducible polynomial $f(x,y)$ with coefficients in $\mathbb{F}_q$ of degree $d>0$ has*

$$N \geq q+1-\frac{1}{2}(d-1)(d-2)\left\lfloor 2q^{\frac{1}{2}}\right\rfloor - d$$

where $N := \#\{(x,y)\in\mathbb{F}_q^2 \mid f(x,y)=0\}$.

Proof. See [28, Corollary 2.b]. □

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

Lemma 73. *The polynomial $f(x,y)=a'x^3-3yx^2+c_1y^3+c_2\in\mathbb{F}_p[x,y]$ has a zero for all prime $p\equiv 1 \bmod 3$ 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 $\deg_x(g(x,y))\geq\deg_x(h(x,y))$, 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 $0\leq i\leq 2$ and $0\leq j\leq 1$, 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

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

with $g_{ij},h_{ij}\in\overline{\mathbb{F}}_p$, 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 lead to the equations

$$g_{02}h_{01}=c_1, \tag{3.5.1}$$
$$g_{01}h_{01}=-g_{02}h_{00}, \tag{3.5.2}$$
$$g_{01}h_{00}=-g_{00}h_{01}, \tag{3.5.3}$$
$$g_{00}h_{00}=c_2. \tag{3.5.4}$$

From (3.5.1) and (3.5.4) it follows that $g_{02}h_{01}\neq 0$ and $g_{00}h_{00}\neq 0$ and, hence, (3.5.1) and (3.5.4) provide

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

which can be insert into (3.5.2) to obtain

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

Inserting all of this in (3.5.3) leads to

$$c_2^2 g_{02}^3 = c_1^2 g_{00}^3. \tag{3.5.5}$$

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, show

$$2g_{02}^3 = -c_1^2 a', \tag{3.5.6}$$

$$c_2^2 a' = g_{00}^3. \tag{3.5.7}$$

By inserting (3.5.7) into (3.5.5) it follows $g_{02}^3 = c_1^2 a'$ which, together with (3.5.6), 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 absolutely 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 72 shows

$$N \geq p - \lfloor 2\sqrt{p} \rfloor - 2.$$

For $p > 7$ it follows that there is a zero of $f(x, y)$. The only prime $p \leq 7$ with $p \equiv 1 \bmod 3$ is 7. 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

$$dx^3 + c_2 \equiv 0 \mod p \tag{3.5.8}$$

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) and at least one of the possible values of d one has $[d] = [c_2]$ 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, hence, 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 74. *The polynomial $f(x, y) = c_1x^3 - 3x + c_2y^3 - 3y + a' \in \mathbb{F}_p[x, y]$ with $p \nmid c_1c_2a'$ is absolutely 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 are polynomials $g(x, y), h(x, y) \in \overline{\mathbb{F}}_p[x, y]$ such that $f(x, y) = g(x, y) \cdot h(x, y)$. One can assume without loss of generality that $\deg_x(g(x, y)) \geq \deg_x(h(x, y))$, 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 $0 \leq i \leq 2$ and $0 \leq j \leq 1$. 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

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

with $g_{ij}, h_{ij} \in \overline{\mathbb{F}}_p$, 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

$$g_{02}h_{01} = c_2, \tag{3.5.9}$$

$$g_{00}h_{00} = a', \tag{3.5.10}$$

$$g_{02}h_{00} + g_{01}h_{01} = 0. \tag{3.5.11}$$

From (3.5.9) and (3.5.10) it follows that $g_{02}h_{01} \neq 0$ and $g_{00}h_{00} \neq 0$, and, hence, one obtains

$$h_{01} = \frac{c_2}{g_{02}}, \qquad h_{00} = \frac{a'}{g_{00}} \qquad \text{and} \qquad g_{01} = -\frac{a'g_{02}^2}{c_2g_{00}}.$$

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

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

These combine 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 absolutely irreducible.

□

Lemma 75. *Let $p \equiv 1 \bmod 3$, $a_1 - a_2 = p^\theta a'$ for some $\theta \in \mathbb{N}$ with $p \nmid a'$, $a_1 \equiv a_2 \equiv 1 \bmod p$, $c_1, c_2, d_1, d_2 \in \mathbb{Z}$ such that $p \nmid c_1 c_2 d_1$, $d_1 \equiv 1 \bmod p$, d_2 is congruent either to 0 or 1 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*

$$\begin{aligned} a_1 x_1^3 + a_2 x_2^3 + p^\theta \left(c_1 y_1^3 + c_2 y_2^3\right) &= 0, \\ x_1 + x_2 + p^\theta \left(d_1 y_1 + d_2 y_2\right) &= 0 \end{aligned}$$

has a non-trivial p-adic solution.

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

$$\begin{aligned} a' x^3 p^\theta + 3a_1 x^2 d p^\theta + 3a_1 x d^2 p^{2\theta} + a_1 d^3 p^{3\theta} + p^\theta \left(c_1 y_1^3 + c_2 y_2^3\right) &= 0, \\ dp^\theta + p^\theta \left(d_1 y_1 + d_2 y_2\right) &= 0. \end{aligned}$$

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

$$\begin{aligned} a' x^3 + 3dx^2 + c_1 y_1^3 + c_2^3 y_2^3 &\equiv 0 \mod p, \\ d + y_1 &\equiv 0 \mod p. \end{aligned}$$

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

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

It follows from Lemma 73 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

$$\begin{aligned} a' + 3d + c_1 y_1^3 + c_2 y_2^3 &\equiv 0 \mod p, \\ d + y_1 + y_2 &\equiv 0 \mod p. \end{aligned} \tag{3.5.12}$$

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

$$a' - 3y_1 - 3y_2 + c_1 y_1^3 + c_2 y_2^3 \equiv 0 \mod p. \tag{3.5.13}$$

If N is the number of solution of this equation, it follows, because the equation is absolutely irreducible due to Lemma 74, with Lemma 72 that

$$N \geq p - \lfloor 2\sqrt{p} \rfloor - 2.$$

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. There are at most six pairs (y_1, y_2) which fulfil this and solve (3.5.13) because the equivalence is fulfilled if

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

which has no solution if $\left(\frac{c_1 c_2}{p}\right) = -1$. If on the other hand $\left(\frac{c_1 c_2}{p}\right) = 1$, it follows that there is a b such that $y_1 \equiv \pm b y_2 \bmod p$. Putting this in (3.5.13), one obtains

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

which has at most three solution in both cases. Hence, if $N > 6$ there is at least one non-trivial p-adic solution. Solving $p - \lfloor 2\sqrt{p} \rfloor - 2 > 6$, one obtains that there are at least seven solutions if $p \geq 17$. The remaining primes for which a non-singular solution of (3.5.13) 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, for fixed values of c_1, c_2, and a', the equation (3.5.13) has a solution which is non-singular as a solution of the system (3.5.12), 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 $c_1, c_2 \in \{1, \ldots, p-1\}$ with $c_1 < c_2$, $[c_1] \neq [c_2]$,$[c_1 - c_2] \neq [a']$ and $a' \in \left\{1, \ldots, \frac{p-1}{2}\right\}$. If $y_i \equiv 0 \bmod p$ and $y_j \not\equiv 0 \bmod p$ for $i, j \in \{1, 2\}$ solve (3.5.13) then this solution is non-singular because one has $c_j y_j^2 - c_i y_i^2 \equiv c_j y_j^2 \not\equiv 0 \bmod p$.

p = 7 By setting either $y_1 = 0$ or $y_2 = 0$, one obtains that if one, c_2 or c_1, 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 also obtains a non-singular solution 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 $y_1 = 0$ or $y_2 = 0$, one obtains that if one, c_2 or c_1, 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 because one has $c_1 y_1^2 - c_2 y_2^2 \not\equiv 0 \bmod p$ in all cases.

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 51 to a non-trivial p-adic solution. □

Lemma 76. *Let $p \equiv 1 \bmod 3$ be a prime. A critical system with $\theta = 3v + r$ where $0 \le r \le 2$, for which $\mu_i > \theta - v$ for $2r + 3 \le i \le 2r + 4$ holds has a non-trivial p-adic solution.*

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

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

where $p^r c_i = a_{2r+2+i}$ and $p^{\theta-v+1}d_i = b_{2r+2+i}$ for $1 \le i \le 2$, hence, the coefficients c_i are not divisible by p. Setting $x_{2r+2+i} = p^v z_i$ for $1 \le i \le 2$, one obtains

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

Due to Conclusion 1 and Lemma 54, 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 modulo p, and they fulfil the equation, it follows that at least two of them are not equivalent to 0 modulo p. After swapping z_1 and z_2 if necessary, one can assume that $z_1 \not\equiv 0 \bmod p$. Set $x_1 = x$ and $x_2 = -x + (-d_1z_1 - d_2z_2)p^{\theta+1}$. Modulo p, the function

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

has 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

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

which proves the claim. □

Lemma 77. *Let $p \equiv 1 \bmod 3$ be a prime. A critical system with $\theta < 3$ has a non-trivial p-adic solution.*

Proof. By the definition of a critical system, it follows that $\theta \ge 1$, hence, the variables $x_{2\theta+3}$ and $x_{2\theta+4}$ are the only ones with the property $\nu_i = \theta$. Suppose that for all $i \in \{2\theta + 3, 2\theta + 4\}$ it holds $\mu_i > \theta$. Then Lemma 76 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 70 gives a non-trivial p-adic solution. It remains the cases with $\mu_i \ge \theta$ for $i \in \{2\theta + 3, 2\theta + 4\}$ and $\mu_i = \theta$ for at least one of them. This case is solved in Lemma 75. □

For the remainder of this section some new notation is needed. For $\tau \in \mathbb{N}_0$, which can be written as $\tau = 3u + \rho$ with $0 \le \rho \le 2$ and $u \in \mathbb{N}_0$, define

$$A(\mathbf{x}) = \sum_{i=1}^{8} a_i x_i^3, \qquad A_\tau(\mathbf{x}) = A(x_1, x_2, p^{u+1}y_0, \dots, p^{u+1}y_\rho, p^u y_{\rho+1}, \dots, p^u y_2),$$
$$B(\mathbf{x}) = \sum_{i=1}^{8} b_i x_i, \qquad B_\tau(\mathbf{x}) = B(x_1, x_2, p^{u+1}y_0, \dots, p^{u+1}y_\rho, p^u y_{\rho+1}, \dots, p^u y_2),$$

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 78. *Let $p \equiv 1 \bmod 3$ be a prime. A critical system with $\mu_i > \nu_i$ for all $i \ge 3$ has a non-trivial p-adic solution.*

Proof. Let $\theta = 3v + r$ with $0 \le r \le 2$. It follows from the definition of $\nu_i^{(\tau)}$ and $\mu_i^{(\tau)}$ that for τ big enough one has $\nu_i^{(\tau)} > \mu_i^{(\tau)}$ for all $i \ge 3$. Let t be the smallest integer possible such that there is an $i \ge 3$ such that $\nu_i^{(t)} \ge \mu_i^{(t)}$. In the case $t > \theta - 3$, it follows from the definition of t that $\nu_i^{(\theta-3)} < \mu_i^{(\theta-3)}$ for all $i \ge 3$. Furthermore, for all $i \in \{2r+3, 2r+4\}$, one has $\nu_i^{(\theta-3)} = \nu_i + 3(v-1+1) = r + 3v = \theta$, $\mu_i^{(\theta-3)} = \mu_i + v - 1 + 1 = \mu_i + v$ and, therefore, $\mu_i > \theta - v$. Hence, Lemma 76 provides a non-trivial p-adic solution. It remains the case with $t \le \theta - 3$. Write $t = 3u' + \rho'$ with $0 \le \rho' \le 2$. As t was chosen smallest possible, it follows that $i \in \{2\rho'+3, 2\rho'+4\}$ for those i with $\mu_i^{(t)} \le \nu_i^{(t)}$. Define

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

For all $i \in \{2\rho'+3, 2\rho'+4\}$, it holds that $\nu_i^{(t)} = \rho' + 3(u'+1) = t+3$, hence, one has $\beta \le t+3 \le \theta$. Writing $\beta = 3u'' + \rho''$ with $0 \le \rho'' \le 2$, 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, $\beta < t+3 \le \theta$. By the minimality of t, it follows that $\nu_{i'}^{(t-1)} < \mu_{i'}^{(t-1)}$. However, one has $\nu_{i'}^{(t)} = \nu_{i'}^{(t-1)} + 3$ and $\mu_{i'}^{(t)} = \mu_{i'}^{(t-1)} + 1$, such that $\nu_{i'}^{(t)} - 3 < \mu_{i'}^{(t)} - 1$ and hence the inequality $t < \beta - 1 < t + 2$ holds, which gives $\beta = t+2$ 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 69 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 $\nu_i^{(t)} \le \mu_i^{(t)}$ with at least one equality and, hence, the system turns into

$$\begin{aligned} a_1 x_1^3 + a_2 x_2^3 + p^{t+3}\left(c_1 x_{2\rho'+3}^3 + c_2 x_{2\rho'+4}^3\right) &= 0, \\ x_1 + \quad x_2 + p^{t+3}\left(d_1 x_{2\rho'+3} + d_2 x_{2\rho'+4}\right) &= 0. \end{aligned}$$

This system has a non-trivial p-adic solution, which follows either by Lemma 75 or Lemma 71.

Now, let $\beta = t+3 = \theta - k$ for $k \in \{1,2\}$. Set everything zero except x_1, x_2, $y_{\rho'}$ and y_r. As before, $\mu_i^{(t)} \geq \nu_i^{(t)}$ 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 distinguishing between the different values of k and ρ'. Let, without loss of generality, be $\mu_{2r+3} \leq \mu_{2r+4}$, hence, one has $\mu_{2r+3}^{(\tau)} \leq \mu_{2r+4}^{(\tau)}$ for all $\tau \in \mathbb{N}_0$. It follows from Lemma 76 that, if no non-trivial p-adic solution exists, $\theta - v \geq \mu_{2r+3}$.

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 applying $y_r \mapsto p^{\theta - v - \mu_{2r+3}} y_r$, one obtains

$$\begin{aligned}\tilde{\nu}_{2r+3}^{(t)} &= \nu_{2r+3}^{(t)} + 3\left(\theta - v - \mu_{2r+3}\right) \geq \nu_{2r+3}^{(t)} + 3 = \theta,\\ \tilde{\mu}_{2r+3}^{(t)} &= \mu_{2r+3}^{(t)} + \theta - v - \mu_{2r+3} = \theta - 1.\end{aligned}$$

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

$$\begin{aligned}a_1x_1^3 + a_2x_2^3 + p^{\theta-1}\left(c_1x_{2\rho'+3}^3 + c_2x_{2\rho'+4}^3\right) + p^\theta \quad dx_{2r+3} &= 0,\\ x_1 + \quad x_2 + p^{\theta-1}\left(d_1x_{2\rho'+3} + d_2x_{2\rho'+4}\right) + p^{\theta-1}ex_{2r+3} &= 0,\end{aligned}$$

with $p \nmid c_1c_2e$, which can be solved with Lemma 69. 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

$$\begin{aligned}a_1x_1^3 + a_2x_2^3 + p^\theta\left(c_1x_{2r+3}^3 + c_2x_{2r+4}^3\right) &= 0,\\ x_1 + x_2 + p^\theta\left(d_1x_{2r+3} + d_2x_{2r+4}\right) &= 0,\end{aligned}$$

with $p \nmid c_1c_2d_1$, which can be solved with Lemma 75.

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 $\mu_{2r+3}^{(t)} = \mu_{2r+3} + v - 1$. Because of $\nu_{2r+3}^{(t)} = \theta - 3$, due to the minimality of t and $\mu_{2r+3} \leq \theta - v$, it follows that

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

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

$$\begin{aligned}a_1x_1^3 + a_2x_2^3 + p^\theta\left(c_1x_{2r+3}^3 + c_2x_{2r+4}^3\right) &= 0,\\ x_1 + x_2 + p^\theta\left(d_1x_{2r+3} + d_2x_{2r+4}\right) &= 0,\end{aligned}$$

with $p \nmid c_1c_2d_1$, which, again, can be solved via Lemma 75. 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 $\tilde{\mu}_{2\rho'+i}^{(t)} \geq \theta - 1$ 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 shape

$$\begin{aligned}a'p^\theta + p^{\theta+1}\left(c_1x_{2\rho'+3}^3 + c_2x_{2\rho'+4}^3\right) + p^\theta \quad \left(e_1x_{2r+3}^3 + e_2x_{2r+4}^3\right) &= 0,\\ p^{\theta-1}\left(d_1x_{2\rho'+3} + d_2x_{2\rho'+4}\right) + p^{\theta-1}\left(f_1x_{2r+3} + f_2x_{2r+4}\right) &= 0,\end{aligned}$$

with $p \nmid c_1c_2d_{2-l}e_1e_2f_1$. Multiplying the cubic equation with $p^{-\theta}$ and the linear one with $p^{-\theta+1}$, one obtains, modulo p, the system

$$\begin{aligned} a' + e_1x_{2r+3}^3 + e_2x_{2r+4}^3 &\equiv 0 \mod p, \\ d_1x_{2\rho'+3} + d_2x_{2\rho'+4} + f_1x_{2r+3} + f_2x_{2r+4} &\equiv 0 \mod p. \end{aligned}$$

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 for $p > 7$ and Lemma 67 for $p = 7$. The linear equation can be solved by setting the remaining variable, which is not $x_{2\rho'+l}$, zero and choosing $x_{2\rho'+l}$ accordingly. This solution is non-singular, because $e_{j-2}x_{2r+j}^2d_{l-2} - pc_{l-2}x_{2\rho'+l}^2f_{j-2} \equiv e_{j-2}x_{2r+j}^2d_{l-2} \not\equiv 0 \bmod p$. Hence, it can be lifted to a non-trivial p-adic solution with Lemma 51. □

Lemma 79. *Let $p \equiv 1 \bmod 3$ be a prime. A critical system with $\theta \geq 5$ has a non-trivial p-adic solution.*

Proof. If $\mu_i > \nu_i$ for all $i \geq 3$, a non-trivial p-adic solution is provided by Lemma 78. If $\mu_i < \nu_i$ for some $i \geq 3$, this is a low variable at a level smaller than θ and, hence, Lemma 70 provides a non-trivial p-adic solution. In the remaining cases, it holds $\mu_i \geq \nu_i$ for all $i \geq 3$ and $\mu_j = \nu_j$ for at least one $j \geq 3$, 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 $j \geq 5$. For this j, it holds $1 \leq \mu_j = \nu_j \leq 2 = 5 - 3 \leq \theta - 3$, hence, Lemma 71 provides a solution. □

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

Lemma 80. *Let $p \equiv 1 \bmod 3$ be a prime. A critical system with $\theta = 4$ has a non-trivial p-adic solution.*

Proof. If $\mu_i > \nu_i$ for all $i \geq 3$, the system can be solved with Lemma 78 and if there is an $i \geq 3$ with $\mu_i < \nu_i$, a non-trivial p-adic solution is provided by Lemma 70. Due to the definition of a critical system, one already knows $\mu_i > \nu_i$ for $3 \leq i \leq 4$. If $\mu_i = \nu_i$ for some $5 \leq i \leq 6$, a solution exists due to Lemma 71. To sum it up, the remaining cases have got $\mu_i > \nu_i$ for $3 \leq i \leq 6$ and at least one of $i \in \{7,8\}$ with $\mu_i = \nu_i$. Without loss of generality, one can assume that $\mu_7 = \nu_7 = 2$, $\mu_8 \geq \nu_8 = 2$ and $\mu_5 \leq \mu_6$. If $\mu_5 > \theta - v = 4 - 1 = 3$, Lemma 76 provides a non-trivial p-adic solution, hence, one can assume $2 \leq \mu_5 \leq 3$. 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 75 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 $\mu_6 \geq \mu_5 = 3$, $\nu_5 = \nu_6 = 4$, $\mu_7 = 3$ and $\nu_7 = 5$. 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

$$\begin{aligned} a' + \tilde{a}_5x_5^3 + \tilde{a}_6x_6^3 &\equiv 0 \mod p, \\ \tilde{b}_5\,x_5 + \tilde{b}_6\,x_6 + \tilde{b}_7x_7 &\equiv 0 \mod p, \end{aligned}$$

with $p \nmid \tilde{a}_5\tilde{a}_6\tilde{b}_5\tilde{b}_7$. Solving the cubic equation modulo p such that $x_i \not\equiv 0 \bmod p$ for some $i \in \{5,6\}$ can be done due to Conclusion 1 and Lemma 67. Then one can use x_7 to solve the linear equation modulo p to obtain a solution which can be lifted to a non-trivial p-adic solution with Lemma 51 because $\tilde{a}_ix_i^2\tilde{b}_7 - p\tilde{a}_7x_7^2\tilde{b}_i \equiv \tilde{a}_ix_i^2\tilde{b}_7 \not\equiv 0 \bmod p$. This solves the case $\theta = 4$. □

Lemma 81. *Let $p \equiv 1 \bmod 3$ be a prime. A critical system with $\theta = 3$ has a non-trivial p-adic solution.*

Proof. If $\mu_i > \nu_i$ for all $i \geq 3$, Lemma 78 provides a non-trivial p-adic solution. Likewise, Lemma 70 provides one if $\mu_i < \nu_i$ for some $i \geq 3$. Without loss of generality, one can assume that $\mu_3 \leq \mu_4$, $\mu_5 \leq \mu_6$ and $\mu_7 \leq \mu_8$. If $\mu_3 > \theta - v = 2$, a non-trivial p-adic solution exists due to Lemma 76, hence, one can assume that $1 \leq \mu_3 \leq 2$.

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 $i \geq 3$ 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 75. Hence, one has $\mu_3 = 1$. 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 69.

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 $\mu_4 \geq \mu_3 = \nu_3 = \nu_4 = \theta$ and, hence, the system can be solved with Lemma 75. For $\mu_3 = 1$, applying $y_0 \mapsto py_0$ and $y_1 \mapsto py_1$ transforms it into a system with $\nu_3 = \nu_4 = \theta$ $\mu_4 \geq \mu_3 = \mu_5 = 2$ and $\nu_5 = 4$. Setting $x_1 = 1$, $x_2 = -1$, $x_6 = x_7 = x_8 = 0$, multiplying the cubic equation with p^{-3} and the linear one with p^{-2}, the systems has, modulo p, the shape

$$\begin{aligned} a' + \tilde{a}_3 x_3^3 + \tilde{a}_4 x_4^3 &\equiv 0 \mod p, \\ \tilde{b}_3 x_3 + \tilde{b}_4 x_4 + \tilde{b}_5 x_5 &\equiv 0 \mod p, \end{aligned}$$

with $p \nmid \tilde{a}_3 \tilde{a}_4 \tilde{b}_3 \tilde{b}_5$. One can solve the cubic equation modulo p such that $x_i \not\equiv 0 \bmod p$ for some $i \in \{3, 4\}$ with Conclusion 1 and Lemma 67. Then one can use x_5 to solve the linear one modulo p. This solution modulo p can be lifted with Lemma 51 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.

3.6 The Cases $(v_0, t) = (4, 3)$ and $(v_0, t) = (4, 4)$

One has to find a non-singular solution of the system

$$\begin{aligned} a_1 x_1^3 + a_2 x_2^3 + a_3 x_3^3 + a_4 x_4^3 &\equiv 0 \mod p, \\ b_1 x_1 + b_2 x_2 + b_3 x_3 + b_4 x_4 &\equiv 0 \mod p, \end{aligned}$$

with $a_1 a_2 a_3 a_4 b_1 b_2 b_3 \not\equiv 0 \bmod p$, 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 51. Applying $x_i \mapsto b_i^{-1} x_i$ for those b_i with $1 \leq i \leq 4$ where $p \nmid b_i$, one can assume that b_i is equivalent to 1 or 0 for $1 \leq i \leq 4$. Starting with the case $(v_0, t) = (4, 3)$, one has to solve the system

$$\begin{aligned} a_1 x_1^3 + a_2 x_2^3 + a_3 x_3^3 + a_4 x_4^3 &\equiv 0 \mod p, \\ x_1 + x_2 + x_3 &\equiv 0 \mod p. \end{aligned} \tag{3.6.1}$$

Due to Lemma 60, 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 $x_4 \not\equiv 0 \bmod p$, one has $a_4 x_4^2 b_1 - a_1 x_1^2 b_4 \equiv a_4 x_4^2 \not\equiv 0 \bmod p$ 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

$$(a_1 - a_3)x_1^3 - 3a_3x_1^2 - 3a_3x_1 + a_2 - a_3 + a_4x_4^3 \equiv 0 \mod p. \tag{3.6.2}$$

There can be at most three solution of (3.6.2) with $x_4 = 0$ because this is a polynomial of degree 3 over a field. Hence, if there are at least four solutions of (3.6.2), at least one of them has to be non-singular. To estimate the number of solution, one can use Lemma 72 again. For that, one needs to show that (3.6.2) is absolutely irreducible. The following lemma provides a way for that.

Lemma 82. *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 [38, Lemma 2C]. □

Lemma 83. *Let $p \equiv 1 \bmod 3$ be a prime. The function $f(x,y) = (a_1 - a_3)x^3 - 3a_3x^2 - 3a_3x + a_2 - a_3 + a_4y^3 \in \mathbb{F}_p[x,y]$ with $p \nmid a_1a_2a_3a_4$ is absolutely irreducible.*

Proof. Define $g(x)$ via

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

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 $1 \leq i \leq 3$ 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 $a_1 = 0$, contradicting the assumption, hence, at least one of the zeros is simple. Therefore, the third equivalence of Lemma 82 is fulfilled and, hence, $a_4^{-1}f(x,y)$ is absolutely irreducible as well as $f(x,y)$. □

Applying Lemma 72 to the function $f(x,y)$, one obtains $N \geq p - \left\lfloor 2\sqrt{p} \right\rfloor - 2$ and, therefore, $N > 3$ for all $p > 11$. It remains to show for $p = 7$ that a solution of the system (3.6.1) 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 (3.6.1) 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 representative of a_i modulo 7 with $1 \leq \tilde{a}_i \leq 6$, 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 $1 \leq l \leq 3$ and multiply the linear equation by -1 to obtain a system as before, where the signs of a_1, a_2 and a_3 have 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 permuting the first three variables if necessary, one obtains a system with $1 \leq \tilde{a}_1 < \tilde{a}_2 \leq 3$ and $\tilde{a}_2 < \tilde{a}_3 \leq 6$.

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

$$\begin{aligned} a_1x_1^3 + a_2x_2^3 + a_3x_3^3 + a_4x_4^3 &\equiv 0 \mod p, \\ x_1 + x_2 + x_3 + x_4 &\equiv 0 \mod p. \end{aligned} \tag{3.6.3}$$

If $a_i \equiv a_j \bmod p$ for some $1 \le i < j \le 4$, the system can be solved due to Lemma 60. 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

$$A_2x_2^3 - 3a\,(1 + x_3)\,x_2^2 - 3a\left(1 + 2x_3 + x_3^2\right)x_2 + A_3x_3^3 - 3ax_3^2 - 3ax_3 + A_1 \equiv 0 \bmod p \tag{3.6.4}$$

or

$$A_2x_2^3 - 3a\,(1 + x_1)\,x_2^2 - 3a\left(1 + 2x_1 + x_1^2\right)x_2 + A_1x_1^3 - 3ax_1^2 - 3ax_1 + A_3 \equiv 0 \bmod p. \tag{3.6.5}$$

The conditions on the a_i transform into $A_i \not\equiv A_j$ for $i \neq j$, $a \not\equiv 0$, $a + A_i \not\equiv 0$ and $A_i \equiv 0$ modulo p for $1 \le i \le 3$. The following lemma shows that at least one of them is absolutely irreducible over $\mathbb{F}_p$.

Lemma 84. *If modulo p one has $A_i \not\equiv A_j$, for $i \neq j$, $a \not\equiv 0$, $a + A_i \not\equiv 0$ and $A_i \not\equiv 0$ for $1 \le i, j \le 3$, at least one of the polynomials*

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

and

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

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

Proof. Let $f(x,y) = Ax^3 - 3a(1+y)x^2 - 3a(1+2y+y^2)x + By^3 - 3ay^2 - 3ay + C$. If $f(x,y)$ is not absolutely irreducible, there are $g(x,y), h(x,y) \in \overline{\mathbb{F}}_p[x,y]$ such that $f(x,y) = g(x,y) \cdot h(x,y)$. Without loss of generality, one can assume that $\deg_x(g(x,y)) \ge \deg_x(h(x,y))$, hence, one has $\deg_x(g(x,y)) = 2$ 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 $0 \le i \le 2$ and $0 \le j \le 1$, which provides the equations

$$\begin{aligned} g_2(y)h_1(y) &= A, \\ g_2(y)h_0(y) + g_1(y)h_1(y) &= -3a\,(1 + y)\,, \\ g_1(y)h_0(y) + g_0(y)h_1(y) &= -3a\left(1 + 2y + y^2\right), \\ g_0(y)h_0(y) &= By^3 - 3ay^2 - 3ay + C, \end{aligned} \tag{3.6.6}$$

where one can compare the degree in y to obtain

$$\begin{aligned} &\deg_y(g_0(y)) = 2, \quad \deg_y(g_1(y)) \in \{0,1\}, \quad \deg_y(g_2(y)) = 0 \\ &\deg_y(h_0(y)) = 1, \quad \deg_y(h_1(y)) = 0, \end{aligned}$$

and hence,

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

with $g_{02}g_{10}g_{20}h_{01}h_{10} \neq 0$ 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 $\deg_y(g_1(y)) = 0$, expanding the left hand side of the first three equations of (3.6.6) 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 (3.6.6) to $9a^2 = AB$. 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 the degree is 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 absolutely irreducible, it follows that $\deg(g_1(y)) = 1$. Here, expanding the left-hand side of the first three of equations (3.6.6) and comparing the coefficients in front of the powers of y gives

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

By combing them with the fourth one, one obtains

$$9a^2 - 9a^2g_{11} + 3aAg_{11} - 6aAg_{11}^2 - A^2g_{11}^3 = AB, \tag{3.6.7}$$
$$9a^2 - 9a^2g_{10} + 3aAg_{10} - 6aAg_{10}^2 - A^2g_{10}^3 = AC, \tag{3.6.8}$$
$$g_{10}\left(-aA + 3a^2 + 4aAg_{11} + A^2g_{11}^2\right) = 9a^2 + aA + 2aAg_{11} - 6a^2g_{11} - 2aAg_{11}^2, \tag{3.6.9}$$
$$g_{11}\left(-aA + 3a^2 + 4aAg_{10} + A^2g_{10}^2\right) = 9a^2 + aA + 2aAg_{10} - 6a^2g_{10} - 2aAg_{10}^2. \tag{3.6.10}$$

Assuming $g_{10} = 0$, the equation (3.6.10) 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, one has $3a - A \neq 0$ and $9a + A \neq 0$. Plugging $g_{11} = \frac{9a+A}{3a-A}$ and $g_{10} = 0$ into (3.6.9) one obtains

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

As 3, a, $9a + A$ and $a + A$ are not zero, it follows that $-3a = A$. Plugging in $g_{10} = 0$ in (3.6.8) 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

$$9a + A + 2Ag - 6ag - 2Ag^2 = 0 \tag{3.6.11}$$

for $g \in \{g_{10}, g_{11}\}$ holds. As both g_{10} and g_{11} are not 0, one can conclude from (3.6.9) and (3.6.10) that

$$-aA + 3a^2 + 4aAg + A^2g^2 = 0. \tag{3.6.12}$$

Combining both equations, one obtains $g = \frac{-6a-A}{2A}$, which plugged into (3.6.12) provides $A = 0$, contradicting the assumption. Hence, $9a + A + 2Ag - 6ag - 2Ag^2 \neq 0$ for $g \in \{g_{10}, g_{11}\}$. Therefore, solving (3.6.9) and (3.6.10) 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}, in terms of the other one. Inserting one into the other, one obtains for $g \in \{g_{10}, g_{11}\}$ the equation

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

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

$$\begin{aligned}&-81a^4 - 36a^3A - 3a^2A^2 + 81a^4g - 54a^3Ag - 24a^2A^2g - aA^3g \\ &+108a^3Ag^2 - 4aA^3g^2 + 54a^2A^2g^3 + 6aA^3g^3 + 12aA^3g^4 + A^4g^4 + A^4g^5 = 0.\end{aligned} \tag{3.6.13}$$

By bringing g^3 to one side of (3.6.7) and (3.6.8) and putting this into (3.6.13), one obtains for $(g, D) \in \{(g_{10}, C), (g_{11}, B)\}$

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

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 (3.6.7) and (3.6.8), provides

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

If one puts this into (3.6.7) and (3.6.8) 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 absolutely 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 absolutely irreducible polynomial. Due to Lemma 72, the number of solution N of this polynomial can be estimated through $N \geq p - \lfloor 2\sqrt{p} \rfloor - 2$. Let $i, j \in \{1,3\}$, $i \neq j$, such that $x_i = 1$ provides an absolutely irreducible polynomial. Then $a_i x_i^2 b_2 - a_2 x_2^2 b_i \equiv a_i - a_2 x_2^2 \bmod p$. If this is not equivalent to 0 modulo p for a solution of the absolutely irreducible polynomial, 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 are 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 absolutely irreducible polynomial. Hence, if there are at least seven solutions of the absolutely irreducible polynomial, at least one does not solve the equation $a_i - a_2 x_2^2 \equiv 0 \bmod p$, proving that it is a one non-singular solution, which can be lifted to a non-trivial p-adic solution, as needed. Therefore, if $p - \lfloor 2\sqrt{p} \rfloor - 2 > 6$, which holds for $p \geq 17$, the case is solved. The cases $p = 7$ and $p = 13$ are handled using the following lemmata.

Lemma 85. *Let $p \equiv 1 \bmod 3$ be a prime. Let $1 \leq i, j, k, l \leq 4$ be all distinct with $[a_i - a_j] = [a_k - a_l]$. Then the system* (3.6.3) *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

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

which can be solved non-trivially due to $[a_i - a_j] = [a_k - a_l]$. Furthermore, one has $a_i x_i^2 b_j - a_j x_j^2 b_i \equiv a_i - a_j \not\equiv 0 \bmod p$ 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 51. □

Lemma 86. *Let $p \equiv 1 \bmod 3$ be a prime. Let $1 \leq i, j, k, l \leq 4$ all distinct with $[a_i] = [a_j]$ and $[a_k] = [a_l]$. Then the system* (3.6.3) *has a non-trivial p-adic solution.*

Proof. As the a_i for $1 \leq i \leq 4$ 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

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

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. By Lemma 51, 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 86, 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 85, 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 $a_2 \leq a_3$. Those cases which cannot be solved with Lemma 85 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
5	8	6	10	1	0	2	5	8	7	3	1	0	9
5	8	10	8	1	0	4	5	12	4	1	1	0	11
5	12	9	5	0	1	7	5	12	11	0	1	5	7
8	12	2	5	1	0	7	8	12	4	3	1	0	9
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 85 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	x_4	a_2	a_3	a_4	x_1	x_2	x_3	x_4
5	2	7	7	1	5	0	8	2	4	5	1	7	0
5	3	6	11	1	1	0	8	3	4	2	1	10	0
5	10	7	8	1	4	0	8	10	7	4	0	3	6
5	11	6	10	1	0	2	8	10	9	0	3	8	2
5	11	9	12	0	2	12	8	11	9	6	1	6	0
12	2	6	11	0	1	1	12	2	9	5	1	0	7
12	3	4	4	1	8	0	12	10	9	10	1	2	0
12	11	4	6	1	0	6	12	11	7	2	1	0	10

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 $1 \leq i \leq 4$, and one $x_j \not\equiv 0 \bmod p$ for $1 \leq j \leq 4$. 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 $p = 3$.

3.7 The Case $p = 3$

As every partial differential of the cubic equation is divisible by 3, one has to find a non-singular solution which solves the cubic equation modulo 9 and the linear one modulu 3, to prove the existence of a non-trivial p-adic solution, as stated in Lemma 51. To show that a non-singular solution for a system (3.3.1) exists, the parameters used in the previous section are not precise enough. Hence, the following notation is required.

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

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

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 (3.3.1) for this proof.

In the proof of Lemma 57, the basics of this idea were already used. By mapping a system (3.3.1) 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 Section 3.3. They map subsets of the set of systems (3.3.1) to the set of systems (3.3.1).

(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 (3.3.1), because if the condition is not fulfilled, then the systems turns into one with non-integer coefficients. A system (3.3.1) 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 (3.3.1) having a confirmed non-trivial 3-adic solution.

The following lemmata proves that systems (3.3.1) with specific parameters have a non-trivial 3-adic solution, which can be combined to show that all ordered conditioned systems (3.3.1) are covered by these systems.

Lemma 87. *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 88. *A system (3.3.1) with $t_{00} + t_{10} + t_{20} \geq 3$ and $1 \leq i < j \leq t_{00}$ 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 zero. Hence, the system (3.3.1) turns into

$$\begin{aligned} a_i x_i^3 + a_j x_j^3 \equiv a_i - a_j &\equiv 0 \mod 9, \\ x_i + x_j \equiv 1 - 1 &\equiv 0 \mod 3. \end{aligned}$$

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 51 provides the wanted solution. □

Lemma 89. *A system (3.3.1) with $t_{00}+t_{10}+t_{20} \geq 1$ and $a_i \equiv a_j \bmod 9$ for some $t_{00}+1 \leq i < j \leq v_0$ has a non-trivial 3-adic solution.*

Proof. Set $x_i = 1$, $x_j = -1$ and the remaining variables zero. 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 51 can be applied to obtain a non-trivial 3-adic solution. □

Lemma 90. *A system (3.3.1) with $t_{00} \geq 5$ 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 88 provides a non-trivial 3-adic solution.

Since $t_{00} \geq 5$ it follows from Lemma 87 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 87 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 zero 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 zero, 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 51. □

By applying transformation (i) to a system (3.3.1) with $t_{10} \geq 5$ it becomes an equivalent system (3.3.1) with $t_{00} \geq 5$.

Conclusion 2. A system (3.3.1) with $t_{10} \geq 5$ has a non-trivial 3-adic solution.

Lemma 91. *An ordered system* (3.3.1) *with* $v_0 \geq 4$ *and* $t_{20} \geq 1$ *has a non-trivial* 3*-adic solution.*

Proof. Choose $x_i \in X_{20}$ and set every variable zero 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 zero. 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 zero. 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 51 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 (3.3.1) with $t_{11} \geq 4$ and $t_{00} \geq 1$ into one with $t_{10} + t_{20} = 0$. Then transformation (iii) can be applied to change it into an system (3.3.1) with $v_0 \geq 4$ and $t_{20} \geq 1$. After renumbering to obtain an ordered system, Lemma 91 provides a non-trivial p-adic solution.

Conclusion 3. A system (3.3.1) with $t_{11} \geq 4$ and $t_{00} \geq 1$ has a non-trivial 3-adic solution.

Lemma 92. *An ordered system* (3.3.1) *with* $v_0 \geq 2$, $v_1 \geq 1$ *and* $t_{20} \geq 1$ *has a non-trivial* 3*-adic solution.*

Proof. Let $x_i \in X_1$ and $x_j \in X_{20}$. Set all variables zero 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 51 to a non-trivial 3-adic one. □

To apply transformation (ii) or (iii) to a system (3.3.1) with $v_0 \geq 1$, $t_{10} \geq 1$ and $t_{21} \geq 2$ or $t_{11} \geq 2$, $t_{21} \geq 1$ and $t_{00} \geq 1$, 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 (3.3.1) with $v_0 \geq 2$, $v_1 \geq 1$ and $t_{20} \geq 1$, which can be renumbered to obtain an ordered system (3.3.1) with the same parameters.

Conclusion 4. A system (3.3.1) with $v_0 \geq 1$, $t_{10} \geq 1$ and $t_{21} \geq 2$ has a non-trivial 3-adic solution.

Conclusion 5. A system (3.3.1) with $t_{11} \geq 2$, $t_{21} \geq 1$ and $t_{00} \geq 1$ has a non-trivial 3-adic solution.

Lemma 93. *A system* (3.3.1) *with* $t_{00} \geq 3$ *and* $t_{11} \geq 1$ *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 88 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 87, $a_i, a_j \in X_{00}$ 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 zero solves the cubic equation modulo 9 and the linear one modulo 3. There is an $x_l \in X_{00}$ which was set zero. The lift of the solution follows by Lemma 51 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 (3.3.1) with $t_{10} \geq 3$ and $t_{21} \geq 1$ it becomes an equivalent system (3.3.1) with $t_{00} \geq 3$ and $t_{11} \geq 1$.

Conclusion 6. A system (3.3.1) with $t_{10} \geq 3$ and $t_{21} \geq 1$ has a non-trivial 3-adic solution.

Lemma 94. *A system* (3.3.1) *with* $t_{01} \geq 2$, $t_{11} \geq 1$ *and* $t_{00} + t_{10} + t_{20} \geq 1$ *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 zero except these three. 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 51. □

By applying transformation (i) to a system (3.3.1) with $t_{11} \geq 2$, $t_{21} \geq 1$ and $t_{10} + t_{20} \geq 1$ it becomes an equivalent system (3.3.1) with $t_{01} \geq 2$, $t_{11} \geq 1$ and $t_{00} + t_{10} + t_{20} \geq 1$.

Conclusion 7. A system (3.3.1) with $t_{11} \geq 2$, $t_{21} \geq 1$ and $t_{10} + t_{20} \geq 1$ has a non-trivial 3-adic solution.

Lemma 95. *A system* (3.3.1) *with* $t_{00} \geq 3$ *and* $t_{01} \geq 2$ *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 88 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 87 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 zero fulfils the cubic congruence modulo 9 and the linear modulo 3. There is an x_m in X_{00} which was set zero. 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 51. □

Apply transformation (i) to a system (3.3.1) with $t_{10} \geq 3$ and $t_{11} \geq 2$. It then becomes an equivalent system (3.3.1) with $t_{00} \geq 3$ and $t_{01} \geq 2$.

Conclusion 8. A system (3.3.1) with $t_{10} \geq 3$ and $t_{11} \geq 2$ has a non-trivial 3-adic solution.

Lemma 96. *An ordered system* (3.3.1) *with* $t_{00} \geq 4$ *and* $t_{10} \geq 1$ *has a non-trivial* 3*-adic solution.*

Proof. One can assume that all a_i with $1 \le i \le t_{00}$ are distinct modulo 9 because otherwise Lemma 88 can be applied to show that there is a non-trivial 3-adic solution.

Permute the first four variables such that $a_1 \equiv \ldots \equiv a_{i_0} \bmod 3$ and $a_1 \not\equiv a_{i_0+1} \equiv \ldots \equiv a_4 \bmod 3$. 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 zero. This solves the cubic equation modulo 9 and the linear one modulo 3. This solution can be lifted by Lemma 51, since $b_3a_1x_1^2 - b_1a_3x_3^2 \equiv a_1 - a_3 \not\equiv 0 \bmod 3$.

Therefore, one can assume that $i_0 \in \{1,3\}$. In this case one of the sets $\{1,4,7\}$ and $\{2,5,8\}$ is completely represented by $a_1,\ldots,a_4$ modulo 9, 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 51 because $a_ix_i^2b_l - a_lx_l^2b_i \equiv a_i \not\equiv 0 \bmod 3$. □

Lemma 97. *An ordered system* (3.3.1) *with* $t_{00} \ge 1$, $t_{01} \ge 3$ *and* $t_{10} \ge 2$ *has a non-trivial* 3*-adic solution.*

Proof. It follows from Lemma 89 that if there are $x_n, x_m \in X_{01}$ with $n \ne m$ and $a_n \equiv a_m \bmod 9$, the system has a non-trivial 3-adic solution. Let $x_i, x_j \in X_{10}$. If $a_i \not\equiv a_j \bmod 9$, set $x_i = -x_j = 1$. Lemma 87 can be applied to show that it is possible to choose $m,n \in X_{01}$ such that $a_m - a_n \equiv a_j - a_i \bmod 9$. Setting $x_m = -x_n = 1$ and the remaining variables zero provides a non-singular solution, because $b_1a_nx_n^2 - b_na_1x_1^2 \equiv a_n \not\equiv 0 \bmod 3$, which can be lifted by Lemma 51 to a non-trivial 3-adic one.

Else $a_i \equiv a_j \bmod 9$. If there is an a_n for $t_{00} + 1 \le n \le v_0$ such that $a_1 + a_i + a_j \equiv \pm a_n \bmod 9$ set $x_1 = x_i = x_j = 1$, $x_n = \mp 1$ and the remaining variables zero. This solves the cubic equation modulo 9 and the linear modulo 3, and can be lifted by Lemma 51, because $b_ia_1x_1^2 - b_1a_ix_i^2 \equiv a_1 \not\equiv 0 \bmod 3$. Else, all a_n for $t_{00} + 1 \le n \le v_0$ 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 $t_{00} + 1 \le n \le v_0$ have to be in the two remaining sets. They are distinct modulo 9, hence, one of the sets is entirely represented. Therefore, there are $t_{00} + 1 \le n < m \le v_0$ with $a_n + a_m \equiv 0 \bmod 9$. Set $x_n = x_m = 1$ and the remaining variables zero. This is a non-singular solution because $b_1a_nx_n^2 - b_na_1x_1^2 \equiv a_n \not\equiv 0 \bmod 3$ and can be lifted to a non-trivial 3-adic solution by Lemma 51, which proves the lemma. □

Lemma 98. *A system* (3.3.1) *with* $t_{01} \ge 4$ *and* $t_{00} + t_{10} + t_{20} \ge 1$ *has a non-trivial* 3*-adic solution.*

Proof. If there are $x_i, x_j \in X_{01}$ with $a_i \equiv a_j \bmod 9$, Lemma 89 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 $x_i \in X_{01}$ completely represented modulo 9. 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 zero provides a non-singular solution, which can be lifted by Lemma 51, because, for $x_l \in X_{00} \cup X_{10} \cup X_{20}$, it follows that $b_la_ix_i^2 - b_ia_lx_l^2 \equiv a_i \not\equiv 0 \bmod 3$. □

By applying transformation (i) to a system (3.3.1) with $t_{11} \ge 4$ and $t_{10} + t_{20} \ge 1$ it becomes a system (3.3.1) with $t_{01} \ge 4$ and $t_{00} + t_{10} + t_{20} \ge 1$.

Conclusion 9. A system (3.3.1) with $t_{11} \geq 4$ and $t_{10} + t_{20} \geq 1$ has a non-trivial 3-adic solution.

Lemma 99. *An ordered system* (3.3.1) *with* $t_{00} \geq 2$, $t_{10} \geq 1$ *and* $t_{11} \geq 1$ *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 $x_{v_0+t_{10}+1} \in \{0, \pm 1\}$ one can solve the cubic equation modulo 9 without changing the value of the linear equation. Setting all remaining variables zero, 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 51. □

Lemma 100. *An ordered system* (3.3.1) *with* $t_{00} \geq 3$, $t_{01} \geq 1$ *and* $t_{10} \geq 2$ *has a non-trivial* 3*-adic solution.*

Proof. One can assume that all a_i with $1 \leq i \leq t_{00}$ are distinct modulo 9, because otherwise Lemma 88 provides a non-trivial 3-adic solution.

Set all variables zero 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 modulo 9, 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, one can assume that 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 $a_i x_i^2 b_{v_0+j} - a_{v_0+j} x_{v_0+j}^2 b_i \equiv a_i \not\equiv 0 \bmod 3$.

For the remaining case $a_{v_0+1} \equiv a_{v_0+2} \bmod 9$ 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. If there is an $i \in \{1, 2, 3\}$ with $x_i \not\equiv 0 \bmod 3$, this solution is 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 equivalence class modulo 3 and $a_{t_{00}+1}$ is 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 zero provides $(A_{\mathbf{x}}, B_{\mathbf{x}}) = (3, 1)$ or $(A_{\mathbf{x}}, B_{\mathbf{x}}) = (6, 1)$, 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 zero gives the desired result. From now on, one can assume without loss of generality that a_1 and a_2 are in the same equivalence class modulo 3 and a_3 is 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 zero 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 proves 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 101. *An ordered system* (3.3.1) *with* $t_{00} \geq 2$, $t_{01} \geq 2$ *and* $t_{10} \geq 2$ *has a non-trivial* 3*-adic solution.*

Proof. Assume $a_{t_{00}+1} \equiv \pm a_{t_{00}+2} \bmod 9$. 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 zero, one obtains a solution of the cubic equation modulo 9 and the linear one modulo 3. The solution is 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 equivalence 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 $a_1 x_1^2 b_{v_0+1} - a_{v_0+1}x_{v_0+1}^2 b_1 \equiv a_1 \not\equiv 0 \bmod 3$ and can be lifted to a non-trivial 3-adic solution with Lemma 51. □

The preceding lemmata and conclusions can be applied to prove Theorem 2 for $p = 3$.

Lemma 102. *An ordered conditioned system with* $s \geq 8$ *has a non-trivial* 3*-adic solution.*

Proof. From the definition of a conditioned system it follows that one with $s \geq 8$ must fulfil

the following four equations:

$$v_0 \geq 3, \tag{3.7.1}$$
$$v_0 + v_1 \geq 6, \tag{3.7.2}$$
$$s = v_0 + v_1 + v_2 \geq 8, \tag{3.7.3}$$
$$t_{00} + t_{10} + t_{20} \geq 1. \tag{3.7.4}$$

Assume there is a conditioned system (3.3.1) with $s \geq 8$ without a non-trivial 3-adic solution.

If this system has $t_{20} \geq 1$, Lemma 91 can be applied to show that $v_0 \leq 3$. From (3.7.1) and (3.7.2), it follows that $v_0 = 3$ and $v_1 \geq 3$, which contradicts Lemma 92. Hence, t_{20} has to be zero.

Lemma 90 can be applied to show that $0 \leq t_{00} \leq 4$. This leaves four cases to consider.

$t_{00} = 0$ If $t_{00} = 0$, it is forced by (3.7.1) that t_{01} is at least 3. Then it follows from Lemma 98 and (3.7.4) that $t_{01} = 3$. Lemma 94 and (3.7.4) can be applied to show that $t_{11} = 0$ and because of (3.7.2) it follows that $t_{10} \geq 3$. At the same time, Conclusion 2 forces t_{10} to be at most 4. Hence, one has $t_{21} \geq 1$, because of (3.7.3), which contradicts Conclusion 6. Therefore, this case cannot occur.

$t_{00} = 1$ One can apply (3.7.1) to show that $t_{01} \geq 2$. This, together with Lemma 98, reveals that $2 \leq t_{01} \leq 3$. Again, Lemma 94 forces t_{11} to be zero. Because of (3.7.2) it follows that t_{10} is at least 2 and, by Conclusion 2, at most 4. Lemma 97 coerces t_{01} to be 2 and, hence, (3.7.3) 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 (3.7.3) to $t_{21} \geq 3$. This contradicts Conclusion 4 and therefore t_{00} cannot be smaller than 2.

$t_{00} = 2$ For $t_{00} = 2$, it follows that $1 \leq t_{01} \leq 3$ because of (3.7.1) and Lemma 98. Hence, (3.7.2) can be applied to show that $v_1 \geq 1$. At this point, further restrictions do not follow from the previous lemmata, hence, another case analysis is necessary.

- **$t_{01} = 3$** Lemmata 94 and 97 restrict t_{11} to be zero and t_{10} to be at most 1. But then one has $t_{10} = v_1$ which has to be at least 1, as proved above. Hence, it follows that $t_{10} = 1$. Then t_{21} is at least 2 because of (3.7.3), which contradicts Conclusion 4.
- **$t_{01} = 2$** Again, Lemma 94 shows that $t_{11} = 0$. But here, (3.7.2) displays that $2 \leq v_1 = t_{10}$, which contradicts Lemma 101.
- **$t_{01} = 1$** Here, (3.7.2) can be applied to show that v_1 is at least 3 and Conclusion 2 to obtain $t_{10} \leq 4$. Unfortunately, this is not enough to conclude anything else and another case analysis is in order.
  - **$t_{10} \geq 3$** It follows from Conclusion 6 that $t_{21} = 0$ and, hence, from (3.7.3) that $v_1 \geq 5$. Hence, one has $t_{11} \geq 1$, which contradicts Lemma 99.
  - **$t_{10} = 2$** By (3.7.2) it follows that t_{11} is at least 1, which contradicts Lemma 99.
  - **$t_{10} = 1$** It follows from (3.7.2) and Conclusion 9 that t_{11} has to be at least 2 and at most 3. This leads, with (3.7.3) which shows that $t_{21} \geq 1$, to a contradiction with Conclusion 7.
  - **$t_{10} = 0$** Here, t_{11} is at least as big as 3 because of (3.7.2). Conclusion 5 can be applied to show that $t_{21} = 0$ and hence $t_{11} \geq 5$ follows by (3.7.3) which contradicts Conclusion 3.

Every case with $t_{00} = 2$ and $t_{01} = 1$ leads to a contradiction, hence, a conditioned system (3.3.1) with $s \geq 8$ 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 exists a non-trivial 3-adic solution, hence, $t_{00} = 2$ cannot occur if such a solution does not exist.

$t_{00} = 3$ It follows from Lemmata 93 and 95 that $t_{11} = 0$ and $t_{01} \leq 1$. Hence, Conclusion 2 and (3.7.2) forces t_{10} to be at least 2 and at most 4. By Conclusion 4, it follows that $t_{21} \leq 1$ and, hence, due to (3.7.3), one obtains $3 \leq t_{10} \leq 4$. Conclusion 6 shows that $t_{21} = 0$ and, hence, again due to (3.7.3), one has $t_{01} = 1$, which contradicts Lemma 100.

$t_{00} = 4$ Again one sees with Lemmata 93 and 95 that $t_{11} = 0$ and $t_{01} \leq 1$. Hence, by (3.7.2), the parameter t_{10} is at least 1 which contradicts Lemma 96.

As shown above, a conditioned system (3.3.1) with $s \geq 8$ which has no non-trivial 3-adic solution cannot have $t_{00} \leq 4$. But as proved before the case analysis those cases with $t_{00} \geq 5$ do have a non-trivial 3-adic solution, hence, the lemma is proved.

□

As discussed at the beginning of this section, this suffices to prove Theorem 2 for $p = 3$. For every other prime the theorem was proved in the previous sections, hence, Theorem 2 holds.

Bibliography

[1] G. I. Arkhipov and A. A. Karatsuba. Local representation of zero by a form. *Izv. Akad. Nauk SSSR Ser. Mat.*, 45(5):948–961, 1198, 1981.

[2] E. Artin. *The collected papers of Emil Artin.* Edited by Serge Lang and John T. Tate. Addison–Wesley Publishing Co., Inc., Reading, Mass.-London, 1965.

[3] J. Ax and S. Kochen. Diophantine problems over local fields. I. *Amer. J. Math.*, 87:605–630, 1965.

[4] J. Browkin. On forms over p-adic fields. *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.*, 14:489–492, 1966.

[5] S. S. Brown. Bounds on transfer principles for algebraically closed and complete discretely valued fields. *Mem. Amer. Math. Soc.*, 15(204):iv+92, 1978.

[6] W. D. Brownawell. On p-adic zeros of forms. *J. Number Theory*, 18(3):342–349, 1984.

[7] J. Brüdern and H. Godinho. On Artin's conjecture. I. Systems of diagonal forms. *Bull. London Math. Soc.*, 31(3):305–313, 1999.

[8] J. Brüdern and H. Godinho. On Artin's conjecture. II. Pairs of additive forms. *Proc. London Math. Soc. (3)*, 84(3):513–538, 2002.

[9] J. Brüdern and O. Robert. On Artin's conjecture: Linear slices of diagonal hypersurfaces. *Trans. Amer. Math. Soc.*, 372(3):1867–1911, 2019.

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

[11] P. J. Cohen. Decision procedures for real and p-adic fields. *Comm. Pure Appl. Math.*, 22:131–151, 1969.

[12] H. Davenport and D. J. Lewis. Homogeneous additive equations. *Proc. Roy. Soc. London Ser. A*, 274:443–460, 1963.

[13] H. Davenport and D. J. Lewis. Simultaneous equations of additive type. *Philos. Trans. Roy. Soc. London Ser. A*, 264:557–595, 1969.

[14] H. Davenport and D. J. Lewis. Two additive equations. In *Number Theory (Proc. Sympos. Pure Math., Vol. XII, Houston, Tex., 1967)*, pages 74–98. Amer. Math. Soc., Providence, R.I., 1969.

[15] V. B. Dem'yanov. On cubic forms in discretely normed fields. *Doklady Akad. Nauk SSSR (N.S.)*, 74:889–891, 1950.

[16] V. B. Dem'yanov. Pairs of quadratic forms over a complete field with discrete norm with a finite field of residue classes. *Izv. Akad. Nauk SSSR. Ser. Mat.*, 20:307–324, 1956.

[17] M. Dodson. Homogeneous additive congruences. *Philos. Trans. Roy. Soc. London Ser. A*, 261:163–210, 1967.

[18] J. H. Dumke. p-adic zeros of quintic forms. *Math. Comp.*, 86(307):2469–2478, 2017.

[19] W. J. Ellison. A 'Waring's problem' for homogeneous forms. *Proc. Cambridge Philos. Soc.*, 65:663–672, 1969.

[20] H. Godinho and T. C. de Souza Neto. Pairs of additive forms of degrees 2.3^τ and 4.5^τ. *J. Comb. Number Theory*, 3(2):87–102, 2011.

[21] H. Godinho and T. C. de Souza Neto. Pairs of additive forms of degree $p^\tau(p-1)$. *Funct. Approx. Comment. Math.*, 48(part 2):197–211, 2013.

[22] H. Godinho, M. P. Knapp, and P. H. A. Rodrigues. Pairs of additive sextic forms. *J. Number Theory*, 133(1):176–194, 2013.

[23] H. Godinho and L. Ventura. Pairs of diagonal forms of degree $3^\tau.2$ and Artin's conjecture. *J. Number Theory*, 177:211–247, 2017.

[24] M. S. Kaesberg. Beyond Artin's conjecture for cubic forms. *Mathematika*, 66(3):577–611, 2020.

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

[26] C. Kränzlein. *Pairs of additive forms of degree* 2^n. PhD thesis, Universität Stuttgart, 2009.

[27] D. B. Leep and W. M. Schmidt. Systems of homogeneous equations. *Invent. Math.*, 71(3):539–549, 1983.

[28] D. B. Leep and C. C. Yeomans. The number of points on a singular curve over a finite field. *Arch. Math. (Basel)*, 63(5):420–426, 1994.

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

[30] D. J. Lewis. Cubic congruences. *Michigan Math. J.*, 4:85–95, 1957.

[31] D. J. Lewis and H. L. Montgomery. On zeros of p-adic forms. *Michigan Math. J.*, 30(1):83–87, 1983.

[32] H. B. Mann and J. E. Olson. Sums of sets in the elementary Abelian group of type (p, p). *J. Combinatorial Theory*, 2:275–284, 1967.

[33] A. Meyer. Mathematische Mittheilungen. *Vierteljahrschrift der Naturforschenden Gesellschaft in Zürich*, 29:209–222, 1884.

[34] L. J. Mordell. A Remark on Indeterminate Equations in Several Variables. *J. London Math. Soc.*, S1-12(1):127.

[35] J. E. Olson. A combinatorial problem on finite Abelian groups. I. *J. Number Theory*, 1:8–10, 1969.

[36] J. E. Olson. A combinatorial problem on finite Abelian groups. II. *J. Number Theory*, 1:195–199, 1969.

[37] S. Poehler. *Two additive quartic forms.* PhD thesis, Universität Stuttgart, 2007.

[38] W. M. Schmidt. *Equations over finite fields. An elementary approach.* Lecture Notes in Mathematics, Vol. 536. Springer-Verlag, Berlin-New York, 1976.

[39] G. Terjanian. Un contre-exemple à une conjecture d'Artin. *C. R. Acad. Sci. Paris Sér. A-B*, 262:A612, 1966.

[40] João Campos Vargas. On artin's conjecture for pairs of diagonal forms. arXiv:2009.13024, 2020.

[41] T. D. Wooley. On simultaneous additive equations. I. *Proc. London Math. Soc. (3)*, 63(1):1–34, 1991.

[42] T. D. Wooley. Artin's conjecture and systems of diagonal equations. *Forum Math.*, 27(4):2259–2265, 2015.

[43] Trevor D. Wooley. Artin's conjecture for septic and unidecic forms. *Acta Arith.*, 133(1):25–35, 2008.

Acknowledgements

I would like to thank all people, who accompanied and supported me during the time of my PhD studies.

First and foremost, I thank my thesis advisor Prof. Dr. Jörg Brüdern for his support and advice. His assistance at every stage of this thesis is greatly appreciated. I am also very grateful to Prof. Dr. Preda Mihăilescu for being my co-referee. Furthermore, I want to thank Prof. Dr. Damaris Schindler, Prof. Dr. Dorothea Bahns, Prof. Dr. Gerlind Plonka-Hoch and Prof. Dr. Anja Sturm for becoming part of the thesis committee.

Many thanks to Knud, whose comments after proofreading parts of my thesis were of great help to me.

I would like to thank my friends and fellow PhD students Eske and Katharina who could always be relied on for discussions - whether the topic was mathematical or non-mathematical.

Finally I want to thank my parents, my sister and my brother for their support and their diversion and my boyfriend Malte, who had to live with me when I was stuck and frustrated but always managed to cheer me up again.