Explicit Local Solubility and Applications

Lea Beneish (University of North Texas),
Christopher Keyes (King's College London)

8 – 15 December 2024

1 Overview of the Field

Let $\mathbb{Q}_p$ denote the field of p-adic numbers and let $K/\mathbb{Q}_p$ be a finite extension with residue field $\mathbb{F}_q$. Artin conjectured that such a K is C_2; that is, for all positive d and all $n \geq d^2$, a homogeneous polynomial $f \in K[x_0, \ldots, x_n]$ of degree d has a nontrivial solution in K. This conjecture was proven false by Terjanian, who found a counterexample with $d = 4$ and $K = \mathbb{Q}_2$ [9]; infinitely many counterexamples have since been found [8].

However, weaker versions of the conjecture are known to hold. For a fixed degree d, we say that K is $C_2(d)$ if for all $n \geq d^2$, every degree d form $f \in K[x_0, \ldots, x_n]$ has a nontrivial solution in K. All p-adic fields K are $C_2(2)$ and $C_2(3)$, due to Hasse and Lewis, respectively [7]. Using techniques from logic, Ax and Kochen showed that p-adic fields are *asymptotically* $C_2(d)$, in the sense that for each d, when the cardinality q of the residue field of K is sufficiently large, we have that K is $C_2(d)$ [1]. In fact, all of the known counterexamples to Artin's conjecture involve composite degrees d, divisible by $q-1$, leaving us with an open conjecture:

Conjecture 1.1 (Artin's conjecture for prime degree p-adic forms)**.** *Let $d > 3$ be prime and $K/\mathbb{Q}_p$ be a finite extension. Then K is $C_2(d)$.*

For small degrees, namely $d = 5, 7, 11$, a p-adic minimization procedure due to Birch and Lewis [2], refined by Laxton and Lewis [5], allows for the reduction to so called *reduced* degree d forms. If f is reduced and q is sufficiently large, an effective version of the Lang–Weil bounds may then be used to produce a nonsingular $\mathbb{F}_q$-solution of $\overline{f}$, which lifts via Hensel's lemma to a K-solution. Refinements of this general strategy have shown that K is $C_2(5)$ whenever $q \geq 11$ (and $C_2(7), C_2(11)$ whenever $q \geq 884, 8054$, respectively). This strategy breaks down for higher (prime) d, since d can be written as the sum of composite numbers, which allows for $\overline{f}$ to have only totally nonreduced and nonlinear components.

2 Recent Developments and Open Problems

We are primarily interested in resolving Conjecture 1.1 or improving the q thresholds for which we know the conjecture to hold for higher d , starting with $d = 5$.

2.1 Quintic forms

The case of quintic forms has a rich history, with several authors contributing to the current state-of-the-art.

Theorem 2.1 (Leep–Yeomans, Heath-Brown, Dumke [6, 4, 3])**.** *Let $d = 5$ and $K/\mathbb{Q}_p$ be a p-adic field with residue field of size q. When $q \geq 11$ we have K is $C_2(5)$.*

Leep and Yeomans refined the p-adic minimization techniques of Birch and Lewis by exploiting the structure of *singular* plane quintic curves to show that when $q \geq 47$, a quintic polynomial over K in 26 or more variables has a solution [6]. The key to their strategy is to carefully argue that if $\overline{f}$ has no nonsingular solutions (which would then be liftable to K by Hensel's lemma), then there exists a plane on which $\overline{f}$ restricts to a quintic curve with at least 3 singularities. The presence of these singularities reduces the q threshold for which explicit point count counting methods guarantee a liftable point.

Later, Heath-Brown recognized that their approach could be combined with a computer search to improve the result to $q \geq 17$ [4]. After a change of coordinates, the plane quintic curves produced by Leep and Yeomans are cut out by one of the following forms

$$t_1 = Ax^3y^2 + Bx^3z^2 + Cy^3z^2 + xyzQ(x, y, z),$$
$$t_2 = Ax^3y^2 + Bx^2z^3 + Cy^3z^2 + xyzQ(x, y, z),$$

where $A, B, C \in \mathbb{F}_q^\times$ and $Q \in \mathbb{F}_q[x, y, z]$ is a quadratic form. A direct computer search shows that for $17 \leq q \leq 43$, all such forms have a nonsingular $\mathbb{F}_q$-solution.

Following a suggestion of Heath-Brown, Dumke extended the approach of Leep and Yeomans to produce singular quintic *surfaces* in $\mathbb{P}^3$ which were amenable to the computational approach of Heath-Brown. These surfaces are cut out by

$$g_1 = a_{01}x_0^3x_1^2 + a_{02}x_0^3x_2^2 + a_{03}x_0^3x_3^2 + a_{12}x_1^3x_2^2 + a_{13}x_1^3x_3^2 + a_{23}x_2^3x_3^2 + \sum_{0\leq i<j<k\leq 3} x_ix_jx_kQ_{ijk}(x_i, x_j, x_k) + x_0x_1x_2x_3L(x_0, x_1, x_2, x_3),$$

or forms g_2, g_3, g_4 of a similar shape, where again the Q_{ijk} are quadratic forms and L is a linear form [3]. While the approach is suitable for $q \geq 7$, the computations proved time-consuming enough that Dumke only computed all such forms for $q \geq 11$.

In order to achieve — or make progress toward — Artin's conjecture for quintic forms, we seek a more streamlined approach that applies to as many q as possible; bespoke methods should only be used when unavoidable, as may be the case for e.g. $q = 2$. We also look to employ parallel computing techniques and the latest hardware improvements, in order to successfully subdue these large search spaces.

2.2 Forms of degree 7

For forms of degree 7, the best available result in the direction of Artin's conjecture is due to Wooley [10].

Theorem 2.2 (Wooley [10])**.** *Let $d = 7$ and $K/\mathbb{Q}_p$ be a p-adic field with residue field of size q. When $q \geq 884$ we have K is $C_2(7)$.*

Wooley's proof of this result does not ensure or exploit any singularities in the relevant degree 7 forms. Instead, he employs an effective version of Bertini's theorem to find planar curves of degree 7 with a non-singular irreducible component of multiplicity one, before applying the Hasse–Weil bounds. Here the worst case is an irreducible smooth curve of degree 7, which is guaranteed to have a point when $q \geq 884$. A similar argument shows $q \geq 8054$ suffices when $d = 11$.

If we were able to carefully slice to produce a planar curve of degree 7 with at least 3 singular points, as Leep and Yeomans did for quintics, we would produce a threshold of $q \geq 587$, improving significantly upon Wooley's result. It remains to be seen whether this is low enough to make explicit computations feasible, as in the quintic case, to lower this bound further.

3 Scientific Progress Made

The headline result of the meeting is the following, extending Theorem 2.1 and marching us ever closer to Artin's conjecture for quintic forms.

Theorem 3.1 (B.–K.)**.** *Let $q \geq 7$ and $K/\mathbb{Q}_p$ be a p-adic field with residue field $\mathbb{F}_q$. Then K is $C_2(5)$.*

3.1 A framework for quintic forms

To prove Theorem 3.1, we develop a framework that generalizes the approaches found in previous work and suggests a blueprint for extending the result to smaller q. The first step is to show, using geometric techniques over finite fields, that if some f has no K-solution, then $\overline{f}$ has at least $k+1$ singular solutions in a particular configuration, starting with $k=2$. With this in hand, we can list all such $\overline{f}$ over $\mathbb{F}_q$ and search for nonsingular solutions; if on all such $\overline{f}$, this search produces a nonsingular solution, then we conclude that K is $C_2(5)$. However, if we find some $\overline{f}$ with only singular solutions, we increment k and begin the process again, hoping to find an eventual contradiction.

Definition. Let $k \geq 1$. A **suspicious k-configuration** is a set of $k+1$ distinct solutions $u_0, \ldots, u_k$ to $\overline{f} = 0$ such that

- $u_0, \ldots, u_k$ are in general position, i.e. they span $\mathbb{P}^k$,
- for all $0 \leq i < j \leq k$, $\overline{f}$ does not vanish on every point of the line between u_i and u_j, and
- $\overline{f}$ has no nonsingular zeros when restricted to the $\mathbb{P}^k$ spanned by $u_0, \ldots, u_k$.

With this definition, an intermediate result of Leep and Yeomans [6, Prop. 5.4], integral to their proof of Theorem 2.1 when $q \geq 47$, can be rephrased as follows: if f has no K-solutions, then there exists a suspicious 2-configuration of solutions to $\overline{f} = 0$. Heath-Brown's approach was then to list all possible such $\overline{f}$ (after suitable change of coordinates) satisfying the first two bullets, and compute directly that when $q \geq 17$, none of them satisfied the last bullet point.

Dumke then went a step further, showing that for $7 \leq q \leq 16$, if f had no K-solutions, then there must exist a suspicious 3-configuration. Critically, this step actually *uses* the computational data from the suspicious 2-configurations, namely that all such $\overline{f}$ vanish on at most 4 (singular) points. For $q = 11, 13, 16$, he then checked all configurations satisfying the first two bullet points (i.e. the $g_1, \ldots, g_4$ mentioned earlier), and found that all had nonsingular points.

One of our key innovations at BIRS was to recognize that we can strengthen these existence results into *extension* results, and then apply this to our proof of Theorem 3.1 in the new cases of $q = 7, 8, 9$. We also strengthen the valid q range for several intermediate steps along the way. One such intermediate step is the following, which is a more flexible generalization of [6, Lemma 5.1].

Lemma 3.2. *Let $q \geq 3$ and $f \in \mathbb{F}_q[x_0, \ldots, x_n]$ be a quintic form. Suppose that U, V are distinct linear spaces of dimension s over $\mathbb{F}_q$ such that f vanishes on U, V and they span $\mathbb{P}^{s+1}$. Then when restricted to the span of U, V, f either*

- *has a nonsingular zero in the span of U, V,*
- *vanishes precisely on U, V, or*
- *vanishes at every point.*

This allows us to prove one of our key ingredients.

Proposition 3.3. *Let $q \geq k+2$ and suppose $f \in K[x_0, \ldots, x_{25}]$ is a reduced quintic form. Suppose $u_0, \ldots, u_k$ are a suspicious k-configuration. Then there exist $\mathbb{F}_q$-solutions $v_0, \ldots, v_{k+1}$ satisfying the first two bullet points of a suspicious $(k+1)$-configuration, such that $\#(\{u_0, \ldots, u_k\} \cap \{v_0, \ldots, v_{k+1}\}) \geq k$.*

When $k = 1$, Proposition 3.3 generalizes [6, Prop. 5.4], and the $k = 2$ version is related to Dumke's work. The $k = 3$ version is entirely novel, and crucial to our proof of Theorem 3.1 for $q = 7$. When q is small, namely $q \in \{2, 3, 4\}$, we are able to produce modified versions, allowing for the possibility that $\overline{f}$ vanishes on a limited number of the lines between v_i, v_j.

3.2 New computations

Leading up to the meeting at BIRS, the second author implemented a parallel search algortithm in C++/CUDA code to be run on a modern GPU, with the goal of extending Dumke's results to $q \leq 9$. With this improved code, we were able to confirm Dumke's work, correct minor errors, and gather data vital to the proof of Theorem 3.1.

When $q = 8$, these computations revealed that there exist no suspicious 3-configurations, thereby proving Theorem 3.1 in this case, when considered together with the propositions above. For $q = 7, 9$, however, a small handful of suspicious 3-configurations were determined to exist! For $q = 9$, these configurations had $\overline{f}$ vanishing on certain lines through the v_i; we are able to exclude this possibility by a minor modification of Proposition 3.3 when $k = 2$ and $q \geq 5$. More subtle was $q = 7$ for which there were three (up to scaling) suspicious 3-configurations; proving Theorem 3.1 in this case requires the $k = 3$ version of Proposition 3.3, together with a careful combinatorial argument, to produce a contradiction, yielding Theorem 3.1.

When $q \leq 5$, these computations produce many (millions, in the case of $q = 5$) of suspicious 3-configurations, putting a similar ad hoc argument out of reach, at least at the present moment.

3.3 Degree 7

We also made progress on the proposed improvements to Wooley's result (Theorem 2.2). A key innovation is a degree 7 analogue of Lemma 3.2.

Even with this, it is not quite so simple as mirroring our approach from the quintic case and looking for a suspicious 2-configuration of $\mathbb{F}_q$-points. In degree 7, this could correspond to $\overline{f}$ cutting out curves with nonreduced components, e.g. a triple line and double quadric. Ruling out these cases remains ongoing work.

4 Outcome of the Meeting

Our meeting at BIRS was highly productive, yielding advances aimed at resolving Artin's conjecture for p-adic forms in degrees 5 and 7. The most notable achievement was the proof of Theorem 3.1, establishing that all p-adic fields with residue field size $q = 7, 8, 9$ are $C_2(5)$. This represents a significant step toward the resolution of the conjecture in the quintic case. Moreover, our approach combining refinements of previous geometric and computational techniques offers the potential to attack the remaining cases of $q \leq 5$.

The meeting also fostered progress on higher-degree forms, particularly for $d = 7$. The development of a degree-7 analogue of Lemma 3.2 lays the groundwork for reducing the threshold for q at which we can prove a p-adic field is $C_2(7)$. While additional work is necessary to complete this process and address further complications, our progress in this direction is cause for optimism at both the possibility of improving on Theorem 2.2, as well as the eventual possibility of bringing this case into a range where we can employ computational strategies.

Other directions for future work include refining our computational techniques, extending our combinatorial framework to higher degrees, and further reducing the thresholds for which we can confirm Artins conjecture. These developments offer insight that we hope will bring us closer to a full resolution of the conjecture.

References

[1] J. Ax and S. Kochen, Diophantine problems over local fields I, *American Journal of Mathematics* **87** (1965), 605–630.

[2] B. J. Birch and D. J. Lewis, $\mathfrak{p}$-adic forms, *The Journal of the Indian Mathematical Society. New Series* **23** (1959), 11–32.

[3] J. H. Dumke, p-adic zeros of quintic forms, *Mathematics of Computation* **86** (2017), 2469–2478.

[4] D. R. Heath-Brown, Zeros of p-adic forms, *Proceedings of the London Mathematical Society* **100** (2010), 560–584.

[5] R. R. Laxton and D. J. Lewis, Forms of degrees 7 and 11 over $\mathfrak{p}$-adic fields. In *Theory of Numbers (A. L. Whiteman, ed.)*, Proceedings of Symposia in Pure Mathematics, **8**, 16–21, American Mathematical Society, 1965.

[6] D. B. Leep and C. C. Yeomans, Quintic forms over p-adic fields, *Journal of Number Theory* **57** (1996), 231–241.

[7] D. J. Lewis, Cubic homogeneous polynomials over $\mathfrak{p}$-adic number fields, *Annals of Mathematics* **56** (1952), 473–478.

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

[9] G. Terjanian, Un contre-exemple à une conjecture d'Artin, *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences. Séries A et B* **262** (1966), A612.

[10] T. D. Wooley, Artin's conjecture for septic and unidecic forms, *Acta Arithmetica* **133** (2008), 25–35.