THE UNIT EQUATION HAS NO SOLUTIONS IN NUMBER FIELDS OF DEGREE PRIME TO 3 WHERE 3 SPLITS COMPLETELY

NICHOLAS GEORGE TRIANTAFILLOU

Abstract. Let K be a number field with ring of integers $\mathcal{O}_K$. We prove that if 3 does not divide $[K : \mathbb{Q}]$ and 3 splits completely in K, then the unit equation has no solutions in K. In other words, there are no $x, y \in \mathcal{O}_K^\times$ with $x + y = 1$. Our elementary p-adic proof is inspired by the Skolem-Chabauty-Coleman method applied to the restriction of scalars of the projective line minus three points. Applying this result to a problem in arithmetic dynamics, we show that if $f \in \mathcal{O}_K[x]$ has a finite cyclic orbit in $\mathcal{O}_K$ of length n then $n \in \{1, 2, 4\}$.

Let K be a number field of degree d over $\mathbb{Q}$ and let $\mathcal{O}_K$ be the ring of integers of K. The set $E_K := \{x \in \mathcal{O}_K^\times : 1 - x \in \mathcal{O}_K^\times\}$ of *exceptional units* in K is well-known to be finite, dating back to Siegel [Sie21]. Each $x \in E_K$ corresponds to a solution in $\mathcal{O}_K^\times$ to the *unit equation*, $x + y = 1$. Solutions to the unit equation and the S-unit equation (which allows x and $1 - x$ to be units up to a fixed-in-advance finite set S of prime ideals) remain of substantial practical interest because of a wide variety of applications to number theory and other fields. These include: enumerating elliptic curves over K with good reduction outside a fixed set of primes [Sma97]; understanding finitely generated groups, arithmetic graphs, and recurrence sequences [EGST88]; and many Diophantine problems [Győ92].

Some work on exceptional units focuses on general upper bounds. Building on work of Baker and Györy on of linear forms in (complex/p-adic) logarithms, Evertse proved an explicit upper bound on $\#E_K$ which is exponential in the degree of K [Eve84]. More recent work (e.g. [Győ19]) has refined these bounds somewhat, but the best known bounds remain exponential, while the 'true' upper bound is conjectured by Stewart to be sub-exponential (see p. 120 of [EGST88].) See [EG15] for more applications and detail on upper bounds.

Other work focuses on low-degree number fields and/or computation. For instance, [Nag70] and [NS98] study the number of exceptional units in fields of degree 3 and 4. There has also been recent progress *computing* the set of solutions to S-unit equations over low-degree number fields [AKM$^+$18] both in practical computation and in the analysis of conjectured p-adic algorithms arising from variants of Chabauty's method [DCW15, Tri20].

Instead of studying low-degree K or general upper bounds, we impose a local condition on K, showing:

Theorem 1. *Let K be a number field. Suppose that $3 \nmid [K : \mathbb{Q}]$ and 3 splits completely in K. Then there is no solution to the unit equation in K. In other words, there is no pair $x, y \in \mathcal{O}_K^\times$ such that $x + y = 1$.*

Remark 2. The set of degree d polynomials in $\mathbb{Z}[x]$ which generate number fields where 3 splits completely have positive density (ordered by height). Indeed, if $g(x) = \sum_{i=0}^d a_i x^i$ satisfies $v_3(a_{d-i}) = i(i-1)/2$ for all i, a Newton polygon computation shows that the roots of g have distinct 3-adic valuations. If g is also irreducible then $\mathbb{Q}[x]/(g(x))$ is a field where 3 splits completely. The set of number fields K where 3 splits completely is expected to have positive density in the set of degree d number fields ordered by discriminant (for any d); there are precise conjectures of what this density should be [Bha07].

Theorem 1 does not give the *first*-known infinite family of number fields of high degree without exceptional units. Indeed, if *any* prime $\mathfrak{p}$ above 2 in K has residue field $\mathbb{F}_\mathfrak{p} \cong \mathbb{F}_2$ then there are no exceptional units in K for a trivial reason. The values x and $1 - x$ cannot simultaneously be non-zero modulo $\mathfrak{p}$. To our knowledge, Theorem 1 yields the first-known infinite family of number fields of high degree without exceptional units outside of these trivial examples.

Remark 3. The hypothesis that $3 \nmid [K : \mathbb{Q}]$ in Theorem 1 is necessary. The set of degree 3 number fields containing exceptional units has been well-understood since at least [Nag70]. One can construct infinitely many degree 3 number fields with an exceptional unit and where 3 splits completely as follows:

Choose an integer $c \equiv 40 \pmod{81}$. Let $g(x) = (x + c)x(x - 1) - 2x + 1$, which is irreducible over $\mathbb{Q}$ be the rational root theorem. Let α be a root of g. Let $K = \mathbb{Q}(\alpha)$. Since $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = -g(0) = -1$ and $\mathrm{Nm}_{K/\mathbb{Q}}(1 - \alpha) = g(1) = -1$, we see that α is an exceptional unit. Since the minimal polynomial of $(\alpha - 2)/3$, namely $\frac{1}{27} g(3x + 2) = x^3 + \frac{c+5}{3} x^2 + \frac{c+2}{3} x + \frac{2c+1}{27}$, has integer coefficients and is congruent to $x(x - 1)(x + 1)$ modulo 3, we see that 3 splits completely in K.

Remark 4. If we replace the hypotheses '$3 \nmid [K : \mathbb{Q}]$ and 3 splits completely in K' with '$5 \nmid [K : \mathbb{Q}]$ and 5 splits completely in K' then Theorem 1 becomes false. Let $g(x) = x^3 - 4x^2 + x + 1$, let α be any root of g, and let $K = \mathbb{Q}(\alpha)$. Then 5 splits completely in K. Moreover, $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = -g(0) = -1$ and $\mathrm{Nm}_{K/\mathbb{Q}}(1 - \alpha) = g(1) = -1$, so α and $1 - \alpha$ are both units, i.e. α is an exceptional unit.

Proof. Suppose that $u, v \in \mathcal{O}_K^\times$ satisfy $-u - v = 1$, so that $-u$ and $-v$ are solutions to the unit equation. Since 3 splits completely in K, there are d embeddings $\mathcal{O}_K \hookrightarrow \mathbb{Z}_3$. Let $u_1, \ldots, u_d$ be the images of u in $\mathbb{Z}_3$ under these embeddings. Since u and v are units, $u_i \in 1 + 3\,\mathbb{Z}_3$ for all $i \in \{1, \ldots, d\}$. Also, $\mathrm{Nm}_{K/\mathbb{Q}}(u), \mathrm{Nm}_{K/\mathbb{Q}}(v) \in$

$\mathbb{Z}^\times = \{\pm 1\}$. We have

$$\prod_{i=1}^{d} u_i = \mathrm{Nm}_{K/\mathbb{Q}}(u) = 1 \qquad \text{and} \qquad \prod_{i=1}^{d}(1+u_i) = \mathrm{Nm}_{K/\mathbb{Q}}(-v) = (-1)^d .$$

We see that $n=1$ is a zero of the 3-adic analytic function

$$f(n) := (1+u_1^n)\cdots(1+u_d^n) - (-1)^d$$

and

$$f(-n) = \prod_{i=1}^{d}(1+u_i^{-n}) - (-1)^d = \prod_{i=1}^{d} u_i^{-n} \prod_{i=1}^{d}(1+u_i^n) - (-1)^d = \prod_{i=1}^{d}(1+u_i^n) - (-1)^d = f(n) .$$

In particular, expanding f as a p-adic power series, all coefficients in odd degrees are zero. Now,

$$f(n) = -(-1)^d + \prod_{i=1}^{d}(1+\exp(n\log u_i)), .$$

Let v_3 be the 3-adic valuation normalized so that $v_3(3)=1$. Since $v_3(\log u_i) \geq 1$ and exp converges when $v_3(n\log u_i) > 1/2$ (see [Gou97]), this expression converges for all $n \in \mathbb{Z}_3$.

Expanding f as a power series,

$$f(n) = -(-1)^d + \prod_{i=1}^{d}\left(2 + n\log u_i + \frac{n^2}{2}(\log u_i)^2 + \frac{n^3}{3!}(\log u_i)^3 + \cdots\right) =: \sum_{j=0}^{\infty} a_j n^j .$$

Now,

$$a_0 = 2^d - (-1)^d , \quad a_1 = 0 , \quad a_2 = 2^{d-3}\sum_{i=1}^{d}(\log u_i)^2 , \quad a_3 = 0 , \quad \text{and} \quad v_3(a_j) \geq 3 \text{ for } j \geq 4 .$$

Since $v_3(a_2) \geq 2$ and $f(1) = 0$ we have $v_3(a_0) \geq 2$. But $v_3(2^d - (-1)^d) \geq 2$ if and only if $3|d$. □

Remark 5. The inspiration for the proof of Theorem 1 is a variant of the method of Skolem-Chabauty-Coleman applied to the *restriction of scalars* of $\mathbb{P}^1_{\mathcal{O}_K} \smallsetminus \{0,1,\infty\}$ from $\mathcal{O}_K$ to $\mathbb{Z}$. In this setting, $\mathbb{P}^1_{\mathcal{O}_K} \smallsetminus \{0,1,\infty\}$ embeds into its *generalized* Jacobian $\mathbb{G}_{m,\mathcal{O}_K} \times \mathbb{G}_{m,\mathcal{O}_K}$ via the Abel-Jacobi map $x \mapsto (x, x-1)$. To prove that $\mathbb{P}^1 \smallsetminus \{0,1,\infty\} = \emptyset$, we consider the restriction of scalars of the Abel-Jacobi map. In this language, the proof of Theorem 1 amounts to showing that for any unit $u \in \mathcal{O}_K^\times$ the intersection

$$E_u := (\mathrm{Res}_{\mathcal{O}_K/\mathbb{Z}}\, \mathbb{P}^1 \smallsetminus \{0,1,\infty\})(\mathbb{Z}_3) \cap \overline{\{u^n : n \in \mathbb{Z}\} \times \mathcal{O}_K^\times}$$

inside $(\mathrm{Res}_{\mathcal{O}_K/\mathbb{Z}}(\mathbb{G}_m \times \mathbb{G}_m))(\mathbb{Z}_3)$ is empty. Here, the closure on the right is respect to the 3-adic topology. To conclude, $\bigcup_{u \in \mathcal{O}_K^\times} E_u = \emptyset$ is the set of solutions to the unit equation in K. See [Tri20] for a more general discussion of using Skolem-Chabauty-Coleman applied to the *restriction of scalars* to compute solutions to the S-unit equation, including a thorough discussion of obstructions to the method arising from unlikely intersections and a conjectural algorithm to compute solutions to the S-unit equation over number fields which do not contain a CM-subfield.

We share an application in arithmetic dynamics communicated to the author by Władysław Narkiewicz.

Corollary 6. *Let K be a number field. Suppose that $3 \nmid [K:\mathbb{Q}]$ and 3 splits completely in K. Suppose that $f \in \mathcal{O}_K[x]$ has a finite orbit of size n in $\mathcal{O}_K$, (i.e., that there exist distinct $a_0, \ldots, a_{n-1} \in \mathcal{O}_K$ such that $f(a_i) = a_{i+1}$ for $i \in \{0, \ldots n-2\}$ and $f(a_{n-1}) = a_0$.) Then, $n \in \{1, 2, 4\}$.*

Proof. Since $\mathcal{O}_K$ embeds in $\mathbb{Z}_3$, the $p = 3$ case of Theorem 2 of [Pez94] says that $n \in \{1, 2, 3, 4, 6, 9\}$. If n is a multiple of 3, replace f with its $(n/3)$ iterate so that f has finite orbit in $\mathcal{O}_K$ of size exactly 3.

Since $(a-b)|(f(a)-f(b))$, it follows that $-\frac{a_1-a_2}{a_0-a_1}, -\frac{a_2-a_0}{a_0-a_1} \in \mathcal{O}_K^\times$. These sum to 1 and are therefore exceptional units. (This observation appears in [NP97].) There are no exceptional units in K, so this is a contradiction, completing the proof.

In fact, it is well-known (and elementary to prove) that there is a polynomial in $\mathcal{O}_K[x]$ with a finite orbit of odd order in $\mathcal{O}_K$ if any only if there is an exceptional unit in K. Using this fact, one can conclude that n is a power of 2 without using the result of Pezda. □

Acknowledgements. Thank you to Joe Rabinoff and Bjorn Poonen for comments which simplified the proof, to Pete Clark, Kálmán Győry, Dino Lorenzini, Władysław Narkiewicz, and Paul Pollack, for helpful feedback on an early draft of this manuscript and to Vishal Arul, Jack Petok, and Padmavathi Srinivasan for helpful conversations. Thank you to the NSF Graduate Research Fellowship under grant #1122374, Simons Foundation grant #550033, and the RTG grant DMS-1344994 in Algebra, Algebraic Geometry, and Number Theory at UGA for funding this work.

References

[AKM+18] Alejandra Alvarado, Angelos Koutsianas, Beth Malmskog, Chris Rasmussen, Christelle Vincent, and Mckenzie West. Solving S-unit equations over number fields. https://trac.sagemath.org/ticket/22148, 2018. 1

[Bha07] Manjul Bhargava. Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants. *International Mathematics Research Notices*, 2007(9):rnm052–rnm052, 2007. 2

[DCW15] Ishai Dan-Cohen and Stefan Wewers. Explicit Chabauty-Kim theory for the thrice punctured line in depth 2. *Proc. Lond. Math. Soc. (3)*, 110(1):133–171, 2015. 1

[EG15] Jan-Hendrik Evertse and Kálmán Győry. *Unit equations in Diophantine number theory*, volume 146. Cambridge University Press, 2015. 1

[EGST88] JH Evertse, K Győry, CL Stewart, and R Tijdeman. S-unit equations and their applications. *New advances in transcendence theory*, pages 110–174, 1988. 1

[Eve84] J.-H. Evertse. On equations in S-units and the Thue-Mahler equation. *Invent. Math.*, 75(3):561–584, 1984. 1

[Gou97] Fernando Q Gouvêa. p-adic numbers. In *p-adic Numbers*, pages 43–85. Springer, 1997. 3

[Győ92] Kálmán Győry. Some recent applications of S-unit equations. *Astérisque*, 209(11):17–38, 1992. 1

[Győ19] Kálmán Győry. Bounds for the solutions of S-unit equations and decomposable form equations ii. *Publ. Math. Debrecen*, 94:507–526, 2019. 1

[Nag70] Trygve Nagell. Quelques problèmes relatifs aux unités algébriques. *Arkiv för Matematik*, 8(2):115–127, 1970. 1, 2

[NP97] Władysław Narkiewicz and Tadeusz Pezda. Finite polynomial orbits in finitely generated domains. *Monatshefte für Mathematik*, 124(4):309–316, 1997. 4

[NS98] Gerhard Niklasch and N Smart. Exceptional units in a family of quartic number fields. *Mathematics of computation*, 67(222):759–772, 1998. 1

[Pez94] Tadeusz Pezda. Polynomial cycles in certain local domains. *Acta Arithmetica*, 66(1):11–22, 1994. 4

[Sie21] Carl Siegel. Approximation algebraischer zahlen. *Mathematische Zeitschrift*, 10(3-4):173–213, 1921. 1

[Sma97] Nigel P Smart. S-unit equations, binary forms and curves of genus 2. *Proceedings of the London Mathematical Society*, 75(2):271–307, 1997. 1

[Tri20] Nicholas Triantafillou. Restriction of scalars Chabauty and the S-unit equation, 2020. 1, 4

N. Triantafillou, Department of Mathematics, University of Georgia, Athens, GA 30602, USA

Email address: `nicholas.triantafillou@uga.edu`