THERE ARE NO EXCEPTIONAL UNITS IN NUMBER FIELDS OF DEGREE PRIME TO 3 WHERE 3 SPLITS COMPLETELY

NICHOLAS 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 there are no exceptional units 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 $n \in \{1, 2, 4\}$.

1. Introduction and Main Result

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]. Let S be a finite set of places of K containing all infinite places. Exceptional units and exceptional S-units (which allow *both* x and $1-x$ to be S-units) 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 [Gyo92].

Date: August 17, 2020.

2010 *Mathematics Subject Classification.* Primary 11D45; Secondary 11D57, 11D88, 11G20.

Key words and phrases. Exceptional units, Skolem's method, Chabauty's method, restriction of scalars.

Thank you to the National Science Foundation Graduate Research Fellowship and Research Training Group in grant in Algebra, Algebraic Geometry, and Number Theory at the University of Georgia [grant numbers 1122374, DMS-1344994]; and the Simons Foundation [grant number 550033] for funding this work.

Each exceptional unit corresponds to a solution in $\mathcal{O}_K^\times$ to a special *unit equation* of the form

$$x + y = 1\,. \tag{1}$$

Unit (resp. S-unit) equations are more general equations of the form

$$ax + by = 1 \tag{2}$$

in units (resp. S-units) of a number field. Several explicit upper bounds have been obtained for the *number* of solutions and for the *heights* of the solutions of (1) and (2). The latter results on the height are effective. Evertse [Eve84] obtained a bound for the number of solutions of (2) which depends only on $s = \#S$. Evertse's bound is exponential in s. The "true" upper bound is conjectured by Stewart to be subexponential (see p. 120 of [EGST88].) The first explicit bounds for the heights of the solutions of (2) were established by Győry [Gyo74] using Baker's method. In terms of S, the best known bounds for the heights of the solutions of (2) are due to [Gyo19].

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. Over low-degree number fields, there has also been recent progress computing the set of solutions to general S-unit equations fields [AKMRVW18] in practice and computing sets of exceptional units a test-case for computations by variants of Chabauty's method [D-CW15, Tri19].

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

Theorem 1.1. *Let K be a number field. Suppose that $3 \nmid [K : \mathbb{Q}]$ and 3 splits completely in K. Then there are no exceptional units in K. In other words, there is no pair $x, y \in \mathcal{O}_K^\times$ such that $x + y = 1$.*

Remark 1.2. 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 1.1 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 1.1 yields the first-known infinite family of number fields of high degree without exceptional units outside of these trivial examples.

Remark 1.3. The hypothesis that $3 \nmid [K : \mathbb{Q}]$ in Theorem 1.1 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 1.4. 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 1.1 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 exceptional units. 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

$$\begin{aligned} f(-n) &= \prod_{i=1}^{d}(1+u_i^{-n}) - (-1)^d \\ &= \prod_{i=1}^{d} u_i^{-n} \prod_{i=1}^{d}(1+u_i^{n}) - (-1)^d \\ &= \prod_{i=1}^{d}(1+u_i^{n}) - (-1)^d \\ &= f(n)\,. \end{aligned}$$

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 with $v_3(3)=1$. 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,

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

We compute

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

Moreover, for all $j \geq 4$, we have $v_3(a_j) \geq 3$. 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 1.5. The inspiration for the proof of Theorem 1.1 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 1.1 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 exceptional units in K. See [Tri19] for a more general discussion of using Skolem-Chabauty-Coleman applied to the restriction of scalars of curves to compute exceptional S-units.

2. An Application of Theorem 1.1

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

Corollary 2.1. *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 $(n/3)$-times 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 Theorem 2 of [Pez94]. ☐

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 earlier drafts of this manuscript and to Vishal Arul, Jack Petok, and Padmavathi Srinivasan for helpful conversations.

References

[AKMRVW18] Alvarado, A., A. Koutsianas, B. Malmskog, C. Rasmussen, C. Vincent, and M. West. "Solving S-unit equations over number fields." SAGE Mathematical Software, 2018. `https://trac.sagemath.org/ticket/22148`

[Bha07] "Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants." *Int. Math. Res. Not. IMRN* 2007, no. 9 (2007): Art. ID rnm052, 20.

[D-CW15] Dan-Cohen, I., and S. Wewers. "Explicit Chabauty-Kim theory for the thrice punctured line in depth 2." *Proc. Lond. Math. Soc. (3)* 110, no. 1 (2015): 133-171.

[Eve84] Evertse, J.-H. "On equations in S-units and the Thue-Mahler equation." *Invent. Math.* 75, no. 3 (1984): 561–584.

[EGST88] Evertse, J. H., K. Győry, C. L. Stewart,and R. Tijdeman. "S-unit equations and their applications." *New advances in transcendence theory* (1988): 110-174.

[Eve15] Evertse, J. H., and K. Győry. *Unit equations in Diophantine number theory.* Vol. 146. Cambridge University Press, 2015.

[Gou97] Gouvêa, Fernando Q. "p-adic Numbers." In *p-adic Numbers*, pp. 43-85. Springer, Berlin, Heidelberg, 1997.

[Gyo74] "Sur les polynômes à coefficients entiers et de discriminant donné II." *Publ. Math. Debrecen*, 21 (1974), 125-144.

[Gyo92] Győry, K. "Some recent applications of S-unit equations." *Astérisque* 209, no. 11 (1992): 17–38.

[Gyo19] Győry, K. "Bounds for the solutions of S-unit equations and decomposable form equations II." *Publ. Math. Debrecen* 94 (2019): 507–526.

[Nag70] Nagell, T. "Quelques problèmes relatifs aux unités algébriques." *Ark. Mat.* 8, no. 2 (1970): 115–127.

[NP97] Narkiewicz W., and T. Pezda. "Finite polynomial orbits in finitely generated domains." *Monatsh. Math.* 124, no. 4 (1997): 309–316

[NS98] Niklasch, G., and N. Smart. "Exceptional units in a family of quartic number fields." *Math. Comp.* 67, no. 222 (1998): 759–772.

[Pez94] Pezda, T. "Polynomial cycles in certain local domains." *Acta Arith.* 66, no. 1 (1994): 11-22.

[Sie21] Seigel, C. "Approximation algebraischer zahlen." *Math. Z.* 10, no. 3–4 (1921): 173–213.

[Sma97] Smart, N. "S-unit equations, binary forms and curves of genus 2." *Proc. Lond. Math. Soc. (3)* 75, no. 2 (1997): 271–307.

[Tri19] Triantafillou, N. "Restriction of Scalars Chabauty and the S-unit equation." arXiv:2006.10590, 2020.

Department of Mathematics, University of Georgia, Athens, GA 30602, USA

Email address: nicholas.triantafillou@uga.edu