PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY, SERIES B
Volume 8, Pages 371–376 (December 22, 2021)
https://doi.org/10.1090/bproc/80

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

NICHOLAS TRIANTAFILLOU

(Communicated by Rachel Pries)

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 [22]. 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/Fermat curves over K with good reduction outside a fixed set of primes [14, 16, 23]; understanding finitely generated groups, arithmetic graphs, and recurrence sequences [7]; and many Diophantine problems [12], including asymptotic versions of Fermat's last theorem [1, 9]. See [8] for many more applications.

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

$$x + y = 1\,. \tag{1.1}$$

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

$$ax + by = 1 \tag{1.2}$$

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 (1.1) and (1.2). The latter results on the height are effective. Evertse [6] obtained a bound

Received by the editors August 17, 2020, and, in revised form, August 29, 2020, September 5, 2020, October 19, 2020, and October 26, 2020.

2020 *Mathematics Subject Classification.* Primary 11D45; Secondary 11D57, 11D88, 11G20.

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

This work was funded by the National Science Foundation Graduate Research Fellowship and Research Training Group 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 the number of solutions of (1.2) which depends only on $s = \#S$. Evertse's bound is exponential in s. The "true" upper bound is conjectured by Stewart to be sub-exponential (see p. 120 of [7].) The first explicit bounds for the heights of the solutions of (1.2) were established by Győry [11] using Baker's method. More recent work has partially replaced the use of Baker's method with Runge's method [15]. Building on this work, the current best bounds (in terms of S) for the heights of the solutions of (1.2) are due to [13].

Other work focuses on low-degree number fields and/or computation. For instance, [18] and [20] study the number of exceptional units in fields of degree 3 and 4. Over low-degree number fields, there has also been recent progress on *computing* the set of solutions to general S-unit equations, building on a long tradition of methods involving Baker's method and/or the theory of linear forms in real, complex, and p-adic logarithms [1].

Yet other work has brought tools from modern number theory to bear. [17], [25], and [26] apply techniques from the theory of modularity to study broad classes of Diophantine equations, yielding efficient algorithms to compute solutions to unit equations using modular symbols. [3], [4], and [5] study unit equations as a test case of Kim's 'nonabelian Chabauty' method for computing integral points. Along similar lines, [24] studies unit equations in order to better understand the power of Chabauty's method for computing integral points in combination with descent by finite covers.

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. (See [2].)

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 [18]. 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 $\mathbb{Q}$ by 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, $\mathrm{Nm}_{K/\mathbb{Q}}(u), \mathrm{Nm}_{K/\mathbb{Q}}(v) \in \mathbb{Z}^\times = \{\pm 1\}$. Combining these facts,

$$\prod_{i=1}^{d} u_i = \mathrm{Nm}_{K/\mathbb{Q}}(u) \in \{\pm 1\} \cap (1 + 3\mathbb{Z}_3) = \{1\} \qquad \text{and}$$

$$\prod_{i=1}^{d} (1+u_i) = \mathrm{Nm}_{K/\mathbb{Q}}(-v) \in \{\pm 1\} \cap (2^d + 3\mathbb{Z}_3) = \{(-1)^d\}.$$

So,

$$\prod_{i=1}^{d} u_i = 1 \qquad \text{and} \qquad \prod_{i=1}^{d} (1+u_i) = (-1)^d.$$

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 in n, 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 [10]), this expression converges for

all $n \in \mathbb{Z}_3$. Expanding f as a power series,

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

Using the fact that f is an even function,

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

We compute

$$a_2 = 2^{d-3}\left(\left(\sum_{i=1}^{d}\log u_i\right)^2 + \sum_{i=1}^{d}(\log u_i)^2\right) = 2^{d-3}\sum_{i=1}^{d}(\log u_i)^2 .$$

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 with respect to the 3-adic topology. To conclude, $\bigcup_{u\in\mathcal{O}_K^\times} E_u = \emptyset$ is the set of exceptional units in K. See [24] 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 [21] 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 [19].) There are no exceptional units in K, so this is a contradiction, completing the proof. □

Remark 2.2. In fact, it is well-known 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. We give a brief proof of this fact below. Using this fact, one can conclude that n is a power of 2 without using Theorem 2 of [21].

Proof of fact. If $u \in \mathcal{O}_K^\times$ is an exceptional unit, then $1-u \in \mathcal{O}_K^\times$ and

$$f(x) = \frac{(x-1)(x-u)}{u} + \frac{ux(x-u)}{1-u} \in \mathcal{O}_K[x]$$

has length 3 orbit $f(0)=1$, $f(1)=u$, and $f(u)=0$.

If some $f \in \mathcal{O}_K[x]$ has an orbit of odd order in $\mathcal{O}_K$, replacing f by an iterate $f \circ \cdots \circ f$, we may assume f has an orbit $a_0, \ldots, a_{p-1} \in \mathcal{O}_K$ of odd *prime* order p. Extending indices cyclicly and applying $(a-b)|(f(a)-f(b))$ repeatedly gives $\frac{a_{j+1}-a_j}{a_{i+1}-a_i} \in \mathcal{O}_K$ for all i and j. Then, for all i, j, k,

$$\frac{a_k - a_j}{a_{i+1}-a_i} = \frac{a_k - a_{k-1}}{a_{i+1}-a_i} + \cdots + \frac{a_{j+1}-a_j}{a_{i+1}-a_i} \in \mathcal{O}_K\,.$$

For any $\ell \not\equiv i \mod p$, we may apply the same argument to the $(\ell - i)$-fold iterate of f to conclude that $\frac{a_k-a_j}{a_\ell - a_i} \in \mathcal{O}_K$. If also $k \not\equiv j \mod p$, the same argument gives $\frac{a_\ell - a_i}{a_k - a_j} \in \mathcal{O}_K$ and so $\frac{a_k-a_j}{a_\ell-a_i} \in \mathcal{O}_K^\times$. Since $p \geq 3$, we may choose i, j, and k which are distinct mod p. Then,

$$\frac{a_k-a_j}{a_k-a_i}, \frac{a_j-a_i}{a_k-a_i} \in \mathcal{O}_K^\times$$

sum to 1 and are therefore exceptional units. □

Acknowledgments

The author thanks Joe Rabinoff and Bjorn Poonen for comments which simplified the proof, to Pete Clark, Kálmán Győry, Dino Lorenzini, Władysław Narkiewicz, Paul Pollack, and the anonymous referees for helpful feedback on earlier drafts of this manuscript and to Vishal Arul, Jack Petok, and Padmavathi Srinivasan for helpful conversations.

References

[1] A. Alvarado, A. Koutsianas, B. Malmskog, C. Rasmussen, C. Vincent, and M. West, *A robust implementation for solving the S-unit equation and several applications*, to appear in *Simons Simp.* `arXiv:1903.00977` 2020.

[2] Manjul Bhargava, *Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants*, Int. Math. Res. Not. IMRN **17** (2007), Art. ID rnm052, 20, DOI 10.1093/imrn/rnm052. MR2354798

[3] David Corwin and Ishai Dan-Cohen, *The polylog quotient and the Goncharov quotient in computational Chabauty–Kim Theory I*, Int. J. Number Theory **16** (2020), no. 8, 1859–1905, DOI 10.1142/S1793042120500967. MR4143688

[4] Ishai Dan-Cohen, *Mixed Tate motives and the unit equation II*, Algebra Number Theory **14** (2020), no. 5, 1175–1237, DOI 10.2140/ant.2020.14.1175. MR4129385

[5] Ishai Dan-Cohen and Stefan Wewers, *Explicit Chabauty-Kim theory for the thrice punctured line in depth 2*, Proc. Lond. Math. Soc. (3) **110** (2015), no. 1, 133–171, DOI 10.1112/plms/pdu034. MR3299602

[6] J.-H. Evertse, *On equations in S-units and the Thue-Mahler equation*, Invent. Math. **75** (1984), no. 3, 561–584, DOI 10.1007/BF01388644. MR735341

[7] J.-H. Evertse, K. Győry, C. L. Stewart, and R. Tijdeman, *S-unit equations and their applications*, New advances in transcendence theory (Durham, 1986), Cambridge Univ. Press, Cambridge, 1988, pp. 110–174. MR971998

[8] Jan-Hendrik Evertse and Kálmán Győry, *Unit equations in Diophantine number theory*, Cambridge Studies in Advanced Mathematics, vol. 146, Cambridge University Press, Cambridge, 2015, DOI 10.1017/CBO9781316160749. MR3524535

[9] Nuno Freitas and Samir Siksek, *The asymptotic Fermat's last theorem for five-sixths of real quadratic fields*, Compos. Math. **151** (2015), no. 8, 1395–1415, DOI 10.1112/S0010437X14007957. MR3383161

[10] Fernando Q. Gouvêa, *p-adic numbers*, 2nd ed., Universitext, Springer-Verlag, Berlin, 1997. An introduction, DOI 10.1007/978-3-642-59058-0. MR1488696

[11] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donné. II*, Publ. Math. Debrecen **21** (1974), 125–144. MR437490

[12] Kálmán Győry, *Some recent applications of S-unit equations*, Astérisque **209** (1992), 11, 17–38. Journées Arithmétiques, 1991 (Geneva). MR1211001

[13] Kálmán Győry, *Bounds for the solutions of S-unit equations and decomposable form equations II*, Publ. Math. Debrecen **94** (2019), no. 3-4, 507–526, DOI 10.5486/pmd.2019.8557. MR3953878

[14] Angelos Koutsianas, *Computing all elliptic curves over an arbitrary number field with prescribed primes of bad reduction*, Exp. Math. **28** (2019), no. 1, 1–15, DOI 10.1080/10586458.2017.1325791. MR3938573

[15] Samuel Le Fourn, *Tubular approaches to Baker's method for curves and varieties*, Algebra Number Theory **14** (2020), no. 3, 763–785, DOI 10.2140/ant.2020.14.763. MR4113780

[16] Beth Malmskog and Christopher Rasmussen, *Picard curves over $\mathbb{Q}$ with good reduction away from 3*, LMS J. Comput. Math. **19** (2016), no. 2, 382–408, DOI 10.1112/S1461157016000413. MR3621646

[17] M. Ram Murty and Hector Pasten, *Modular forms and effective Diophantine approximation*, J. Number Theory **133** (2013), no. 11, 3739–3754, DOI 10.1016/j.jnt.2013.05.006. MR3084298

[18] Trygve Nagell, *Quelques problèmes relatifs aux unités algébriques* (French), Ark. Mat. **8** (1969), 115–127, DOI 10.1007/BF02589552. MR268154

[19] W. Narkiewicz and T. Pezda, *Finite polynomial orbits in finitely generated domains*, Monatsh. Math. **124** (1997), no. 4, 309–316, DOI 10.1007/BF01319041. MR1480362

[20] G. Niklasch and N. P. Smart, *Exceptional units in a family of quartic number fields*, Math. Comp. **67** (1998), no. 222, 759–772, DOI 10.1090/S0025-5718-98-00958-2. MR1464147

[21] T. Pezda, *Polynomial cycles in certain local domains*, Acta Arith. **66** (1994), no. 1, 11–22, DOI 10.4064/aa-66-1-11-22. MR1262650

[22] Carl Siegel, *Approximation algebraischer Zahlen* (German), Math. Z. **10** (1921), no. 3-4, 173–213, DOI 10.1007/BF01211608. MR1544471

[23] N. P. Smart, *S-unit equations, binary forms and curves of genus* 2, Proc. London Math. Soc. (3) **75** (1997), no. 2, 271–307, DOI 10.1112/S002461159700035X. MR1455857

[24] Nicholas George Triantafillou, *Restriction of Scalars, the Chabauty-Coleman Method, and*, ProQuest LLC, Ann Arbor, MI, 2019. Thesis (Ph.D.)–Massachusetts Institute of Technology. MR4051431

[25] Rafael von Känel, *Integral points on moduli schemes of elliptic curves*, Trans. London Math. Soc. **1** (2014), no. 1, 85–115, DOI 10.1112/tlms/tlu003. MR3296485

[26] R. von Känel and B. Matschke, *Solving S-unit, Mordell, Thue, Thue—Mahler and generalized Ramanujan—Nagell equations via Shimura—Taniyama conjecture*, `arXiv:1605.06079`, 2016, accepted at Mem. Amer. Math. Soc.

Department of Mathematics, University of Georgia, Athens, Georgia 30602
Email address: `nicholas.triantafillou@uga.edu`