Algebra & Number Theory

Volume 15
2021
No. 10

The unit equation over cyclic number fields of prime degree

Nuno Freitas, Alain Kraus and Samir Siksek

msp

ALGEBRA AND NUMBER THEORY 15:10 (2021)
https://doi.org/10.2140/ant.2021.15.2647

The unit equation over cyclic number fields of prime degree

Nuno Freitas, Alain Kraus and Samir Siksek

Let $\ell \neq 3$ be a prime. We show that there are only finitely many cyclic number fields F of degree ℓ for which the unit equation

$$\lambda + \mu = 1, \qquad \lambda, \mu \in \mathcal{O}_F^\times$$

has solutions. Our result is effective. For example, we deduce that the only cyclic quintic number field for which the unit equation has solutions is $\mathbb{Q}(\zeta_{11})^+$.

1. Introduction

Let F be a number field. Write $\mathcal{O}_F$ for the integers of F, and $\mathcal{O}_F^\times$ for the unit group of $\mathcal{O}_F$. A famous theorem of Siegel [1929] asserts that the *unit equation*,

$$\lambda + \mu = 1, \qquad \lambda,\ \mu \in \mathcal{O}_F^\times, \tag{1-1}$$

has finitely many solutions. Unit equations have been the subject of research for over a century. Effective bounds for the number and heights of the solutions have been supplied by many authors [Evertse and Győry 2015, Chapter 4]. One of the most elegant such results is due to Evertse [1984], and asserts that (1-1) has at most $3 \times 7^{3r+4s}$ solutions, where (r, s) is the signature of F. The latest effective bounds on the heights of solutions are due to Győry [2019]. Moreover, de Weger [1989] has given a rather efficient algorithm for determining the solutions to (1-1) which combines Baker's bounds for linear forms in logarithms with the LLL algorithm. De Weger's algorithm has since been refined by a number of authors, for example [Alvarado et al. 2019; von Känel and Matschke 2016; Smart 1998]. A related problem (with connections to Lehmer's Mahler measure conjecture) is to study, for a unit α of infinite order, the number of integers n such that $1 - \alpha^n$ is also a unit. This problem is considered by Silverman [1995] who shows that the number of such n is $O(d^{1+7/\log\log d})$ where d is the degree of $\mathbb{Q}(\alpha)$.

It is natural to consider the existence of solutions to (1-1). Nagell [1969b] called a unit $\lambda \in \mathcal{O}_F^\times$ *exceptional* if $1 - \lambda \in \mathcal{O}_F^\times$. The number field F is called *exceptional* if it possesses an exceptional unit. Thus λ is exceptional if and only if $(\lambda, 1 - \lambda)$ is a solution to the unit equation (1-1), and F is exceptional

Freitas is supported by a Ramón y Cajal fellowship with reference RYC-2017-22262. Siksek is supported by the EPSRC grant *Moduli of Elliptic curves and Classical Diophantine Problems* (EP/S031537/1).
MSC2020: 11R20.
Keywords: unit equation, cyclic fields, exceptional fields.

if and only if the unit equation has solutions. In a series of papers spanning over 40 years, starting with [Nagell 1928] and culminating in [Nagell 1969a], Nagell determined all exceptional number fields where the unit rank is 0 or 1. For example, Nagell [1969a, Section 2] found that the only exceptional quadratic fields are $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{-3})$ which contain exceptional units $(1+\sqrt{5})/2$ and $(1-\sqrt{-3})/2$ respectively, and the only exceptional complex cubic fields are the ones with discriminants -23 and -31. Nagell [1969a, Sections 3–5] also showed that the only exceptional real cubic fields (whence the unit rank is 2) are of the form $\mathbb{Q}(\lambda)$, where λ is a root of

$$f_k(X) = X^3 + (k-1)X^2 - kX - 1, \qquad k \in \mathbb{Z}, \quad k \geq 3$$

or of

$$g_k(X) = X^3 + kX^2 - (k+3)X + 1, \qquad k \in \mathbb{Z}, \quad k \geq -1;$$

in both cases λ is an exceptional unit. It turns out the fields $\mathbb{Q}(\lambda)$ defined by the $f_k(X)$ are non-Galois, whereas the ones defined by the $g_k(X)$ are cyclic (and so Galois), having discriminant $(k^2+3k+9)^2$. By a *cyclic* number field we mean a finite Galois extension of $\mathbb{Q}$ whose Galois group is cyclic.

An interesting problem is determining whether a family of number fields has exceptional members. Beyond the work of Nagell, there are relatively few works on this problem. A beautiful example of such a result is due to Triantafillou [2020]: if 3 totally splits in a number field F and $3 \nmid [F:\mathbb{Q}]$ then F is nonexceptional. Another example of such a result is found in [Freitas et al. 2020]: if F is a Galois p-extension, where $p \geq 5$ is a prime that totally ramifies in F, then F is nonexceptional.

In this note we consider the problem of determining exceptional number fields that are cyclic of prime degree.

Theorem 1. *Let $\ell \neq 3$ be a prime. Then there are only finitely many cyclic number fields F of degree ℓ such that F is exceptional.*

For $\ell = 2$ the theorem is due to Nagell [1969a] who showed, as observed above, that the only exceptional quadratic fields are $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{-3})$. For $\ell = 3$ the theorem is false. Indeed, as already observed the fields defined by the polynomials g_k are cyclic cubic and exceptional, and Nagell [1969a, Théorème 7] showed that this family contains infinitely many pairwise nonisomorphic members. For $\ell \geq 5$, Theorem 1 is an immediate consequence of the following more precise theorem.

Theorem 2. *Let $\ell \geq 5$ be a prime, and write*

$$R_\ell = \mathrm{Res}(X^{2\ell}-1, (X-1)^{2\ell}-1), \tag{1-2}$$

where Res *denotes the resultant. Then $R_\ell \neq 0$. Let*

$$S_\ell = \{p \mid R_\ell \,:\, p \text{ is a prime} \equiv 1 \pmod{\ell}\}. \tag{1-3}$$

Let F be a cyclic number field of degree ℓ, and suppose the unit equation (1-1) has solutions. Write Δ_F for the discriminant of $\mathcal{O}_F$, and N_F for the conductor of F. Then there is a nonempty subset $T \subseteq S_\ell$ such that

$$\Delta_F = \prod_{p \in T} p^{\ell-1}, \qquad N_F = \prod_{p \in T} p. \tag{1-4}$$

We recall that the *conductor* of a finite abelian extension $F/\mathbb{Q}$ is the smallest n such that $F \subseteq \mathbb{Q}(\zeta_n)$, where $\zeta_n = \exp(2\pi i/n)$. Theorem 2 is effective, in the sense that given a prime $\ell \geq 5$, it gives an effective algorithm for determining all exceptional cyclic number fields of degree ℓ. Indeed, the theorem yields a finite list of cyclic fields of degree ℓ that could be exceptional, and for each such cyclic field we can simply solve the unit equation using de Weger's aforementioned algorithm to decide if it exceptional or not. We illustrate this by establishing the following corollary.

Corollary 1. *The only exceptional cyclic quintic field is* $F = \mathbb{Q}(\zeta_{11})^+$.

The proof of Corollary 1 is found in Section 5.

Remark. Let $\mathcal{F}$ be the collection of all exceptional cyclic fields of prime degree $\neq 3$. It is natural in view of the above results to wonder if $\mathcal{F}$ is finite or infinite. We believe that $\mathcal{F}$ is infinite, as we now explain. First let $p \geq 5$ be a prime, and let $F = \mathbb{Q}(\zeta_p)^+$. We will show that F is exceptional by exhibiting a solution to the unit equation (1-1). Let $\lambda = 2 + \zeta_p + \zeta_p^{-1}$ and $\mu = -1 - \zeta_p - \zeta_p^{-1}$. Then λ, μ belong to $\mathcal{O}_F$ and satisfy $\lambda + \mu = 1$. We need to show that λ, μ are units in $\mathcal{O}_F$ and for this it is in fact enough to show that they are units in $\mathbb{Z}[\zeta_p]$. Recall that the unique prime ideal above p in $\mathbb{Z}[\zeta_p]$ is generated by $1 - \zeta_p^j$, where j is any integer $\not\equiv 0 \pmod p$, and thus the ratio $(1 - \zeta_p^j)/(1 - \zeta_p^k)$ is a unit for any pair of integers $j, k \not\equiv 0 \pmod p$. Note that

$$\lambda = (1 + \zeta_p)(1 + \zeta_p^{-1}) = \frac{(1 - \zeta_p^2)(1 - \zeta_p^{-2})}{(1 - \zeta_p)(1 - \zeta_p^{-1})}, \qquad \mu = -\zeta_p^{-1}(1 + \zeta_p + \zeta_p^2) = -\zeta_p^{-1}\frac{(1 - \zeta_p^3)}{(1 - \zeta_p)},$$

showing that λ, μ are units. Hence $F = \mathbb{Q}(\zeta_p)^+$ is exceptional for all $p \geq 5$. Note that F is cyclic of degree $(p-1)/2$. Recall that a *Sophie Germain prime* is a prime ℓ such that $p = 2\ell + 1$ is also prime. For any Sophie Germain prime $\ell \geq 5$, the number field $F = \mathbb{Q}(\zeta_p)^+$ with $p = 2\ell + 1$ is an exceptional cyclic field of degree ℓ and so belongs to $\mathcal{F}$. It is conjectured that there are infinitely many Sophie Germain primes [Shoup 2009, page 123], and this conjecture would imply that $\mathcal{F}$ is infinite.

We thank the referees for their comments.

2. Ramification in cyclic fields of prime degree

Lemma 1. *Let ℓ be a prime. Let F be a cyclic number field of degree ℓ. Write Δ_F for the discriminant of $\mathcal{O}_F$. Let p be a prime that ramifies in F. Then the following hold.*

(i) *p totally ramifies in F.*

(ii) *If $p \neq \ell$ then* $\operatorname{ord}_p(\Delta_F) = \ell - 1$.

Proof. Let $I \subseteq \operatorname{Gal}(F/\mathbb{Q})$ be an inertia subgroup for p. Since p ramifies, $I \neq 1$. As $\operatorname{Gal}(F/\mathbb{Q})$ has prime order, $I = \operatorname{Gal}(F/\mathbb{Q})$. Hence p is totally ramified in F, and we can write $p\mathcal{O}_F = \mathfrak{p}^\ell$ where $\mathfrak{p}$ is the unique prime ideal above p.

We now prove (ii). Suppose $p \neq \ell$, therefore p is tamely ramified in F. Write $\mathfrak{D}_F$ for the different ideal for the extension $F/\mathbb{Q}$. As the ramification degree is ℓ, we conclude [Neukirch 1999, page 199] that $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{D}_F) = \ell - 1$. However [Neukirch 1999, page 201], the discriminant and different are related by $|\Delta_F| = \mathrm{Norm}_{F/\mathbb{Q}}(\mathfrak{D}_F)$. Hence $\mathrm{ord}_p(\Delta_F) = \ell - 1$. This completes the proof. □

Lemma 2. *Let m, n be positive integers with $m \mid n$. Let ℓ be a prime and let F be a cyclic number field of degree ℓ. If $F \subseteq \mathbb{Q}(\zeta_n)$ and $\ell \nmid [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_m)]$ then $F \subseteq \mathbb{Q}(\zeta_m)$.*

Proof. Suppose $F \subseteq \mathbb{Q}(\zeta_n)$ but $F \not\subseteq \mathbb{Q}(\zeta_m)$. As F has prime degree ℓ we have $F \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$. Thus $[F \cdot \mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m)] = [F : \mathbb{Q}] = \ell$. However, $\mathbb{Q}(\zeta_m) \subseteq F \cdot \mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_n)$. Therefore $\ell \mid [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_m)]$, giving a contradiction. □

Lemma 3. *Let ℓ be a prime and let F be a cyclic number field of degree ℓ. Suppose $\ell \nmid \Delta_F$. Then the conductor of F is squarefree, and divisible only by primes $p \equiv 1 \pmod{\ell}$.*

Proof. Let n be the conductor of F. The primes that ramify in F are precisely the primes dividing the conductor [Neukirch 1999, Corollary VI.6.6]. As $\ell \nmid \Delta_F$ we see that $\ell \nmid n$.

We would like to show that n is squarefree. Suppose that n is not squarefree. Then we may write $n = p^r n'$ where p is a prime, $r \geq 2$, and $p \nmid n'$. Let $m = pn'$. We denote Euler's totient function by φ. Then

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_m)] = \frac{\varphi(n)}{\varphi(m)} = \frac{(p-1)p^{r-1}\varphi(n')}{(p-1)\varphi(n')} = p^{r-1}.$$

This is not divisible by ℓ and so by Lemma 2, $F \subseteq \mathbb{Q}(\zeta_m)$. But $m < n$, contradicting the fact that n is the conductor of F. It follows that n is squarefree.

Next let $p \mid n$ and write $n = pm$ with $p \nmid m$. Then

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_m)] = p - 1.$$

By Lemma 2 and the definition of conductor we have $\ell \mid (p-1)$. □

3. The unit equation and ramification

We now prove one of the claims in Theorem 2.

Lemma 4. *Let $\ell \neq 3$ be a prime. Let R_ℓ be given by (1-2), then $\ell \nmid R_\ell$. In particular, $R_\ell \neq 0$.*

Proof. Suppose $\ell \mid R_\ell$. Then the polynomials $X^{2\ell} - 1$ and $(X-1)^{2\ell} - 1$ have a common root $\theta \in \overline{\mathbb{F}}_\ell$. But in $\mathbb{F}_\ell[X]$ we have

$$X^{2\ell} - 1 = (X^2 - 1)^\ell = (X-1)^\ell (X+1)^\ell, \qquad (X-1)^{2\ell} - 1 = \big((X-1)^2 - 1\big)^\ell = X^\ell (X-2)^\ell.$$

Hence $\theta \in \{1, -1\} \cap \{0, 2\} \subset \mathbb{F}_\ell$. As $\ell \neq 3$ this intersection is empty, giving a contradiction, so $\ell \nmid R_\ell$. □

Remark. Lemma 4 is false for $\ell = 3$. Indeed, $(1 + \sqrt{-3})/2$ is a common root to $X^6 - 1$ and $(X-1)^6 - 1$, thus $R_3 = 0$.

For the remainder of this section F will be a cyclic number field of prime degree $\ell \geq 5$. By Lemma 1, every rational prime p which ramifies in F is in fact totally ramified, and so there is a unique prime $\mathfrak{p}$ of F above p. The prime $\mathfrak{p}$ must have inertial degree 1, and so $\mathcal{O}_F/\mathfrak{p} \cong \mathbb{F}_p$.

Lemma 5. *Let $\lambda \in \mathcal{O}_F^\times$. Let $b \in \mathbb{Z}$ satisfy $\lambda \equiv b \pmod{\mathfrak{p}}$. Then $b^\ell \equiv \pm 1 \pmod{p}$.*

Proof. As $\mathfrak{p}$ is the unique prime above p we have $\mathfrak{p}^\sigma = \mathfrak{p}$ for all $\sigma \in G = \mathrm{Gal}(F/\mathbb{Q})$. Applying σ to $\lambda \equiv b \pmod{\mathfrak{p}}$ gives $\lambda^\sigma \equiv b \pmod{\mathfrak{p}}$. Hence

$$\pm 1 = \mathrm{Norm}_{F/\mathbb{Q}}(\lambda) = \prod_{\sigma \in G} \lambda^\sigma \equiv b^\ell \pmod{\mathfrak{p}}.$$

Since b^ℓ is a rational integer, $b^\ell \equiv \pm 1 \pmod{p}$. □

Lemma 6. *Suppose the unit equation (1-1) has a solution. Let R_ℓ be as in (1-2). Then every prime p ramifying in F satisfies $p \mid R_\ell$.*

Proof. Let (λ, μ) be a solution to the unit equation. Let p be a prime ramifying in F and let $\mathfrak{p}$ be the prime above it. Write $\lambda \equiv b \pmod{\mathfrak{p}}$ and $\mu \equiv c \pmod{\mathfrak{p}}$ with $b, c \in \mathbb{Z}$. By Lemma 5, $b^{2\ell} \equiv 1 \pmod{p}$ and $c^{2\ell} \equiv 1 \pmod{p}$. However, $\lambda + \mu = 1$. Hence $c \equiv 1 - b \pmod{p}$. Therefore $(b-1)^{2\ell} = (1-b)^{2\ell} \equiv c^{2\ell} \equiv 1 \pmod{p}$. Hence, the polynomials $X^{2\ell} - 1$ and $(X-1)^{2\ell} - 1$ have a common root in $\mathbb{F}_p$, showing that $p \mid R_\ell$. □

4. Proof of Theorem 2

We now prove Theorem 2. Thus let F be a cyclic number field of prime degree $\ell \geq 5$ such that the unit equation (1-1) has solutions. Let R_ℓ be given by (1-2). From Lemma 4 we know that $R_\ell \neq 0$. Let S_ℓ be given by (1-3).

Claim. *Every prime p ramified in F belong to S_ℓ.*

Proof. First note that every ramified p divides R_ℓ by Lemma 6. Next note that $\ell \nmid R_\ell$ by Lemma 4. Thus ℓ is unramified in F, and so $\ell \nmid \Delta_F$. Now Lemma 3 tells us that every ramified $p \equiv 1 \pmod{\ell}$. This completes the proof of the claim. □

Let T be the set of primes dividing the discriminant Δ_F. This is also the set of primes dividing the conductor N_F (see for example [Neukirch 1999, Corollary VI.6.6]). We know from the claim that T is a subset of S_ℓ. Moreover, by a famous theorem of Minkowski [Neukirch 1999, Theorem III.2.17] there are no number fields of discriminant ± 1, and thus $T \neq \varnothing$.

Next, by part (ii) of Lemma 1, and Lemma 3, we have

$$\Delta_F = g \cdot \prod_{p \in T} p^{\ell - 1}, \qquad N_F = \prod_{p \in T} p, \tag{4-1}$$

where $g = \pm 1$. However, as F is Galois of odd degree, it is totally real, and therefore the discriminant is positive, so $g = 1$. This completes the proof.

field	defining polynomial
$F_{11} = \mathbb{Q}(\zeta_{11})^+$	$x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1$
F_{31}	$x^5 - x^4 - 12x^3 + 21x^2 + x - 5$
$F_{341,1}$	$x^5 + x^4 - 136x^3 - 300x^2 + 2016x + 3136$
$F_{341,2}$	$x^5 + x^4 - 136x^3 + 41x^2 + 3039x + 1431$
$F_{341,3}$	$x^5 + x^4 - 136x^3 + 723x^2 - 1053x + 67$
$F_{341,4}$	$x^5 + x^4 - 136x^3 - 641x^2 - 371x + 67$

Table 1. Cyclic number fields F with conductor dividing $341 = 11 \times 31$.

5. Proof of Corollary 1

Let F be an exceptional cyclic quintic field. We apply Theorem 2 with $\ell = 5$. Then

$$R_5 = \mathrm{Res}(X^{10} - 1, (X-1)^{10} - 1) = -210736858987743 = -3 \times 11^9 \times 31^3.$$

Thus $S_5 = \{11, 31\}$. We obtain three possibilities for the conductor N_F: $11, 31, 341 = 11 \times 31$. Thus F is a degree 5 subfield of $\mathbb{Q}(\zeta_{11})$, $\mathbb{Q}(\zeta_{31})$ or $\mathbb{Q}(\zeta_{341})$. These respectively have Galois groups isomorphic to $\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/30\mathbb{Z}$ and $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$. By the Galois correspondence, $\mathbb{Q}(\zeta_{11})$ and $\mathbb{Q}(\zeta_{31})$ both have a unique subfield of degree 5, which we denote by $F_{11} = \mathbb{Q}(\zeta_{11})^+$ and F_{31}. The group $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ has six subgroups of index 5, and so we obtain six subfields of $\mathbb{Q}(\zeta_{341})$ of degree 5. However, two of these are F_{11} and F_{31}, so we only obtain four new fields which we denote by $F_{341,1}$, $F_{341,2}$, $F_{341,3}$, $F_{341,4}$. We found defining polynomials for all these number fields in [Jones and Roberts 2014], which we reproduce in Table 1.

We used the unit equation solver in the computer algebra package `Magma` [Bosma et al. 1997]. This is an implementation of the de Weger algorithm for solving unit equations with improvements due to Smart [1998]. Applying the solver to our six number fields we find that the unit equation (1-1) does not have solutions for $F = F_{31}$ and $F = F_{341,i}$ with $i = 1, \dots, 4$. It does however have 570 solutions for $F = F_{11} = \mathbb{Q}(\zeta_{11})^+$.

References

[Alvarado et al. 2019] 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", 2019. arXiv

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR Zbl

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

[Evertse and Győry 2015] J.-H. Evertse and K. Győry, *Unit equations in Diophantine number theory*, Cambridge Studies in Advanced Mathematics **146**, Cambridge Univ. Press, 2015. MR Zbl

[Freitas et al. 2020] N. Freitas, A. Kraus, and S. Siksek, "On asymptotic Fermat over $\mathbb{Z}_p$-extensions of $\mathbb{Q}$", *Algebra Number Theory* **14**:9 (2020), 2571–2574. MR Zbl

[Győry 2019] K. Győry, "Bounds for the solutions of S-unit equations and decomposable form equations II", *Publ. Math. Debrecen* **94**:3-4 (2019), 507–526. MR

[Jones and Roberts 2014] J. W. Jones and D. P. Roberts, "A database of number fields", *LMS J. Comput. Math.* **17**:1 (2014), 595–618. MR Zbl

[von Känel and Matschke 2016] R. von Känel and B. Matschke, "Solving S-unit, Mordell, Thue, Thue–Mahler and generalized Ramanujan–Nagell equations via Shimura–Taniyama conjecture", 2016. arXiv

[Nagell 1928] T. Nagell, "Darstellung ganzer Zahlen durch binäre kubische Formen mit negativer Diskriminante", *Math. Z.* **28**:1 (1928), 10–29. MR Zbl

[Nagell 1969a] T. Nagell, "Quelques problèmes relatifs aux unités algébriques", *Ark. Mat.* **8** (1969), 115–127. MR Zbl

[Nagell 1969b] T. Nagell, "Sur un type particulier d'unités algébriques", *Ark. Mat.* **8** (1969), 163–184. MR Zbl

[Neukirch 1999] J. Neukirch, *Algebraic number theory*, Grundl. Math. Wissen. **322**, Springer, 1999. MR Zbl

[Shoup 2009] V. Shoup, *A computational introduction to number theory and algebra*, 2nd ed., Cambridge Univ. Press, 2009. MR Zbl

[Siegel 1929] C. L. Siegel, "Über einige Anwendungen diophantischer Approximationen", *Abh. Preuß. Akad. Wiss.* **1929**:1 (1929), 1–41.

[Silverman 1995] J. H. Silverman, "Exceptional units and numbers of small Mahler measure", *Experiment. Math.* **4**:1 (1995), 69–83. MR Zbl

[Smart 1998] N. P. Smart, *The algorithmic resolution of Diophantine equations*, London Mathematical Society Student Texts **41**, Cambridge Univ. Press, 1998. MR Zbl

[Triantafillou 2020] N. Triantafillou, "The unit equation has no solutions in number fields of degree prime to 3 where 3 splits completely", 2020. arXiv

[de Weger 1989] B. M. M. de Weger, *Algorithms for Diophantine equations*, CWI Tract **65**, Stichting Math. Centrum, Amsterdam, 1989. MR Zbl

Communicated by Bjorn Poonen
Received 2020-12-11 Revised 2021-03-13 Accepted 2021-04-15

nunobfreitas@gmail.com — *Department de Matemàtiques i Informàtica, Universitat de Barcelona, Barcelona, Spain*

alain.kraus@imj-prg.fr — *Institut de Mathématiques de Jussieu - Paris Rive Gauche, Sorbonne Université, UMR 7586 CNRS - Paris Diderot, Paris, France*

s.siksek@warwick.ac.uk — *Mathematics Institute, University of Warwick, Coventry, United Kingdom*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2021 is US \$415/year for the electronic version, and \$620/year (+\$60, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 15 No. 10 2021