Alabama Journal of Mathematics
41 (2017)

ISSN 2373-0404

Units in Quadratic and Multi-Quadratic Fields

Adam A. Pratt
Department of Mathematics
University of Illinois at Chicago

Maria E. Stadnik
Department of Mathematical Sciences
Florida Atlantic University

Mary-Stewart Wachter
Department of Geosciences
Mississippi State University

In this paper, we investigate multi-quadratic fields, looking for those that contain units of norm -1. We provide results concerning the existence of units of norm -1 in fields of the form $\mathbb{Q}(\sqrt{2p})$ for prime $p \equiv 1 \mod 4$ and prove that all of the fields $\mathbb{Q}(\sqrt{2}, \sqrt{p})$ with $p \equiv 5 \mod 8$ prime contain a unit of norm -1.

Introduction and Motivation

An example of a question in number theory that is fairly easy to state (but has no easy solution) is Artin's conjecture on primitive roots. An integer a is a primitive root mod p if $\langle a \rangle = (\mathbb{Z}/p\mathbb{Z})^\times$, that is, if a is a generator for the multiplicative group of integers mod p. Artin's conjecture on primitive roots states that given an integer $a \neq \pm 1$ or a square, there exist infinitely many primes p (or, a positive density of primes in the set of all primes) such that a is a primitive root mod p Artin (1965). The conjecture was posed by Emil Artin in 1927; it is still unresolved today. However, there has been significant progress on a proof; it is known to be true given the truth of a set of the generalized Riemann hypotheses (GRH) Hooley (1967), and it has been proven that Artin's conjecture holds for infinitely many a Gupta and Murty (1984).

The conjecture has been generalized in a variety of ways and interesting results have been proven, many assuming the truth of a set of generalized Riemann hypotheses. One way to generalize it is to consider a number field besides the rational numbers. For a number field K, we may substitute the integers with the ring of integers of the field, O_K, replace $\langle a \rangle$ with any multiplicative subgroup of $K^\times$, and ask an analogous question. For example, given the field $K = \mathbb{Q}[\sqrt{2}]$, its ring of integers, $O_K = \mathbb{Z}[\sqrt{2}]$, and the group of units $O_K^\times = \{\pm(1+\sqrt{2})^n : n \in \mathbb{Z}\}$, one may ask for which primes p is the image of $O_K^\times$ in $(O_K/pO_K)^\times$ maximized. This generalization of Artin's conjecture has been proven to hold true for a real quadratic or multi-quadratic field (assuming a set of the generalized Riemann hypotheses) if and only if the field contains a unit of norm -1Roskam (2000); Stadnik (2017). This leads us to explore when quadratic and multi-quadratic fields have units of norm -1, which is the focus of this article.

Finding a unit of norm -1 in the quadratic field $\mathbb{Q}(\sqrt{d})$ is equivalent to finding integer solutions (x, y) to the negative Pell equation $x^2 - dy^2 = -1$ (or more generally $x^2 - dy^2 = -4$). We prove in Theorem 3.1 that a set of fields of the form $\mathbb{Q}(\sqrt{2p})$ have a unit of norm -1, and in Theorem 4.2 we show that all fields $\mathbb{Q}(\sqrt{2}, \sqrt{p})$ with $p \equiv 5 \mod 8$ prime contain a unit of norm -1.

Background

Our main objects of study are number fields, which are finite field extensions of the rational numbers $\mathbb{Q}$. The simplest type of number field is a quadratic field, which is a field of the form $\mathbb{Q}(\sqrt{d})$ for a square free integer d. More generally, a *multi-quadratic field* is a field of the form $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_n})$ where d_i is square free for each $1 \leq i \leq n$ and $n \in \mathbb{Z}$.

Definition 1. *Let $K \subseteq F$ be a finite field extension, and let $\alpha \in F$. We can view F as a vector space over K. The norm of α, $N_{F/K}(\alpha)$, is the determinant of the linear transformation of F given by multiplication by α Fröhlich and Taylor (1991).*

Given any number field, there is a ring associated to it that is the analog of the integers $\mathbb{Z}$. The *ring of integers*, O_K, of a number field K is the set of all $\alpha \in K$ that satisfies a polynomial of the form $x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ where $a_i \in \mathbb{Z}$ for $0 \leq i \leq n-1$. By abuse of notation, we call units in the ring of integers O_K of a number field K the *units of K*.

Corresponding Author Email: mstadnik@fau.edu

Proposition 1. *If E is a field containing a unit of norm -1, then every subfield $F \subseteq E$ also contains a unit of norm -1.*

Proof. Let E be a field with a unit α satisfying $N_{E/\mathbb{Q}}(\alpha) = -1$. Then $N_{E/\mathbb{Q}}(\alpha) = N_{F/\mathbb{Q}} \circ N_{E/F}(\alpha) = -1$ since the norm map is multiplicative Ireland and Rosen (1990). Thus for $\beta = N_{E/F}(\alpha)$, it is clear that $N_{F/\mathbb{Q}}(\beta) = N_{F/\mathbb{Q}}(N_{E/F}(\alpha)) = -1$. □

Thus, it makes sense to begin our search for units of norm -1 in multi-quadratic fields by examining units in their subfields, which are also multi-quadratic fields. The most basic nontrivial subfields of multi-quadratic fields are quadratic fields. Even for these fields, a complete list of which have a unit of norm -1 has not been determined. It is known Fröhlich and Taylor (1991) that when $p \equiv 1 \mod 4$ is prime, the field $\mathbb{Q}(\sqrt{p})$ has a unit of norm -1, and if $p, q \equiv 1 \mod 4$ are prime numbers satisfying the Legendre symbol $\left(\frac{p}{q}\right) = -1$ (that is, $p \equiv x^2 \mod q$ has no solution in the integers), then $\mathbb{Q}(\sqrt{pq})$ contains a unit of norm -1 (Ireland and Rosen (1990), Ch. 17). By contrast, if there is a prime divisor $p|d$ such that $p \equiv 3 \mod 4$, then $\mathbb{Q}(\sqrt{d})$ has no unit of norm -1 Fröhlich and Taylor (1991).

If $K = \mathbb{Q}(\sqrt{d})$ and $d \equiv 2, 3 \mod 4$, then $O_K = \mathbb{Z}[\sqrt{d}]$ and the norm of $\alpha = a + b\sqrt{d}$ for integers a and b is $N_{K/\mathbb{Q}}(\alpha) = a^2 - b^2 d$ Fröhlich and Taylor (1991). Hence finding units of norm -1 in K is equivalent to finding solutions to the equation $x^2 - dy^2 = -1$ in the integers. An equation of the form $x^2 - dy^2 = 1$ for $d > 0$ and square free with solutions (x, y) in the integers is known as a Pell's equation, and the similar equation $x^2 - dy^2 = -1$ is known as a negative Pell's equation. It is known Ireland and Rosen (1990) that there are infinitely many solutions to each Pell's equation; the smallest positive solution is known as the *fundamental solution.* It is still an open question to determine for precisely which d the negative Pell's equation $x^2 - dy^2 = -1$ has infinitely many solutions, but we see the connection between finding a unit of norm -1 in these quadratic fields and finding solutions to a negative Pell's equation.

If $K = \mathbb{Q}(\sqrt{d})$ and $d \equiv 1 \mod 4$, then $O_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ and the norm of $\alpha = a + b\left(\frac{1+\sqrt{d}}{2}\right) \in O_K$ is $N_{K/\mathbb{Q}}(\alpha) = a^2 + ab + b^2\left(\frac{1-d}{4}\right)$. Completing the square and multiplying by 4, we determine that a unit $\alpha = a + b\left(\frac{1+\sqrt{d}}{2}\right)$ of norm -1 in K is an integer solution to $-4 = (2a+b)^2 - b^2 d$.

Results for Quadratic Fields

Starting with a field of the form $\mathbb{Q}(\sqrt{2p})$, $p \equiv 1 \mod 4$, we find that not every such field contains the unit of norm -1. The smallest counterexample is $\mathbb{Q}(\sqrt{34})$. In Mollin and Srinivasan (2010), it is proven that the negative Pell's equation $x^2 - ny^2 = -1$ has a solution in the case that $a \equiv -1 \mod 2n$, where (a, b) is the fundamental solution to the positive Pell's equation $x^2 - ny^2 = 1$. A solution (u, v) to the equation $x^2 - ny^2 = -1$ for $n = 2p$ then can be used to form the unit $u + v\sqrt{2p} \in \mathbb{Q}(\sqrt{2p})$ that has norm -1 by construction, proving the following theorem.

Theorem 1. *Consider, for p prime, the quadratic field $\mathbb{Q}(\sqrt{2p})$. Let (a, b) be the fundamental solution to the positive Pell's Equation $x^2 - 2py^2 = 1$. If $a \equiv -1 \mod 4p$, then the field has a unit of norm -1.*

Results for Multi-Quadratic Fields

We continue the search for units of norm -1 in higher degree multiquadratic fields, beginning with biquadratic fields, i.e. those of the form $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. This type of field has three quadratic subfields, namely $Q_1 = \mathbb{Q}(\sqrt{d_1})$, $Q_2 = \mathbb{Q}(\sqrt{d_2})$, and $Q_3 = \mathbb{Q}(\sqrt{d_1 d_2})$. Fields of this type have been extensively studied in the literature, and various results have been proven that we find useful. Kuroda's class number formula for multiquadratic fields relates units of K with units and class numbers of subfields (see Kuroda (1950) or Wada (1966)).

Theorem 2. ***(Kuroda's class number formula for biquadratic fields)*** *Let K denote a totally real biquadratic field with quadratic subfields Q_1, Q_2, and Q_3. Let h_i denote the class number of Q_i, let h denote the class number of K, and let $O_{Q_i}^\times$ be the group of units of Q_i. Then*

$$h = 1/4 \cdot \left[O_K^\times : \prod_{i=1}^{3} O_{Q_i}^\times \right] h_1 h_2 h_3.$$

In Kubota (1956), Kubota completely classified the structure of the unit group of a biquadratic field K into one of seven types. His work proves that if each quadratic subfield of K has a unit $x_i \in Q_i$ of norm $N_{\mathbb{Q}}^{Q_i} x_i = -1$, then a system of fundamental units of K must be of one of the two forms $\{\epsilon_1, \epsilon_2, \epsilon_3\}$ or $\left\{\epsilon_1, \epsilon_2, \sqrt{\epsilon_1\epsilon_2\epsilon_3}\right\}$.

By Proposition 2.2, it is necessary that each of Q_1, Q_2, and Q_3 has a unit of norm -1. In general this is not a sufficient condition; for example, $\mathbb{Q}(\sqrt{10}, \sqrt{17})$ has no unit of norm -1 even though its three quadratic subfields $\mathbb{Q}(\sqrt{10})$, $\mathbb{Q}(\sqrt{17})$, and $\mathbb{Q}(\sqrt{170})$ all do. It is known that if p, $q \equiv 1 \mod 4$ are primes with Legendre symbol $\left(\frac{p}{q}\right) = -1$, then the multi-quadratic field $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ contains a unit of norm -1 Kubota (1956). A proof of this fact in English is provided in the Appendix. Attempting to generalize this result, we consider fields of the form $K = \mathbb{Q}(\sqrt{2}, \sqrt{p})$ for $p \equiv 1 \mod 4$ prime, $(\frac{2}{p}) = -1$. Since , $(\frac{2}{p}) = -1$ if and only if $p \equiv 3, 5 \mod 8$ and $\mathbb{Q}(\sqrt{p})$ has no unit of norm -1

when $p \equiv 3 \mod 8$, we turn our attention to primes $p \equiv 5 \mod 8$. It turns out that all of these fields contain a unit of norm -1.

Theorem 3. *Suppose $p \equiv 5 \mod 8$ is prime. Then $K = \mathbb{Q}(\sqrt{2}, \sqrt{p})$ contains a unit of norm -1.*

Proof. Let K be as given and let $Q_1 = \mathbb{Q}(\sqrt{2})$, $Q_2 = \mathbb{Q}(\sqrt{p})$, and $Q_3 = \mathbb{Q}(\sqrt{2p})$ be the three quadratic subfields of K. We have seen that each Q_i has fundamental unit ϵ_i of norm -1. So, from Kubota's work, we know the unit group of K has one of the two systems of fundamental units $\{\epsilon_1, \epsilon_2, \epsilon_3\}$ or $\left\{\epsilon_1, \epsilon_2, \sqrt{\epsilon_1\epsilon_2\epsilon_3}\right\}$. K has the former structure if and only if $\left[O_K^\times : \prod_{i=1}^3 O_{Q_i}^\times\right] = 1$ and K has no unit of norm -1; K has the latter structure if and only if $\left[O_K^\times : \prod_{i=1}^3 O_{Q_i}^\times\right] = 2$ and $z = \sqrt{\epsilon_1\epsilon_2\epsilon_3}$ is a unit in K of norm -1. We will show that a system of fundamental units for K is the latter structure, so K contains a unit z of norm -1.

Let h_i denote the class number of Q_i and let h denote the class number of K. Clearly $h_1 = 1$, as $\mathbb{Z}[\sqrt{2}]$ is a principal ideal domain. Since $p \equiv 1 \mod 4$, genus theory tells us that h_2 is odd, and in Kučera (1995) it is proven that $h_3 \equiv 2 \mod 4$. By Kuroda's class number formula for biquadratic fields, $h = 1/4 \cdot \left[O_K^\times : \prod_{i=1}^3 O_{Q_i}^\times\right] h_1 h_2 h_3 \in \mathbb{N}$, so it must be that $2 \left| \left[O_K^\times : \prod_{i=1}^3 O_{Q_i}^\times\right]\right.$. Thus the unit group of K must have system of fundamental units given by $\left\{\epsilon_1, \epsilon_2, \sqrt{\epsilon_1\epsilon_2\epsilon_3}\right\}$, implying that K contains a unit of norm -1.

□

The next two corollaries follow directly from Theorem 4.2 and Stadnik (2017).

Corollary 1. *The generalization of Artin's conjecture on primitive roots holds for fields of the form K as defined above (assuming the truth of the GRH).*

Corollary 2. *There is a positive density of primes p for which the generalization of Artin's conjecture on primitive roots holds for fields of the form $K = \mathbb{Q}(\sqrt{2}, \sqrt{p})$ (assuming the truth of the GRH).*

It should be noted that there are fields of the form $K = \mathbb{Q}(\sqrt{2}, \sqrt{p})$ for $p \equiv 1 \mod 8$ that contain a unit of norm -1; one such example is $\mathbb{Q}(\sqrt{2}, \sqrt{113})$. If $p \equiv 3$ or $7 \mod 8$, then the field $\mathbb{Q}(\sqrt{2}, \sqrt{p})$ will not contain a unit of norm -1 since the subfield $\mathbb{Q}(\sqrt{p})$ will not contain a unit of norm -1.

We search for examples of higher degree multi-quadratic fields that contain units of norm -1 utilizing the computer algebra system PARI/gp. We consider fields of the form $\mathbb{Q}(\sqrt{5}, \sqrt{p}, \sqrt{q})$, specifically looking at fields satisfying $\left(\frac{5}{p}\right), \left(\frac{5}{q}\right), \left(\frac{p}{q}\right) = -1$, as these are good candidates for fields with units of norm -1 by Proposition 2.2. We find many examples, the smallest being $\mathbb{Q}(\sqrt{5}, \sqrt{13}, \sqrt{37})$. We also investigate extension fields of $\mathbb{Q}$ of degree 16. One example we find is $\mathbb{Q}(\sqrt{5}, \sqrt{17}, \sqrt{97}, \sqrt{853})$.

Further Research

Based on computations using PARI/gp, we conjecture that fields of the form $K = \mathbb{Q}(\sqrt{2}, \sqrt{p}, \sqrt{q})$ contain a unit of norm -1 if both $\mathbb{Q}(\sqrt{2p}, \sqrt{q})$ and $\mathbb{Q}(\sqrt{2q}, \sqrt{p})$ contain a unit of norm -1 (for $p, q \equiv 1 \mod 4$ prime and $\left(\frac{p}{q}\right) = -1$). This conjecture holds for all of the fields we tested, though some of those positive results depend on the truth of GRH. We also want to look for trends to determine when fields of the form $\mathbb{Q}(\sqrt{2p}, \sqrt{q})$ contain a unit of norm -1 when $p, q \equiv 1 \mod 4$ and $\left(\frac{p}{q}\right) = -1$ (not all of them do).

Appendix

Theorem 4. *Suppose $p, q \equiv 1 \mod 4$ are prime numbers satisfying $\left(\frac{p}{q}\right) = -1$. Then $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ contains a unit of norm -1.*

Proof. Let K be as given and let $Q_1 = \mathbb{Q}(\sqrt{p})$, $Q_2 = \mathbb{Q}(\sqrt{q})$, and $Q_3 = \mathbb{Q}(\sqrt{pq})$ be the three quadratic subfields of K. From (Fröhlich and Taylor (1991), Ireland and Rosen (1990), Ch. 17), it is known that each Q_i has fundamental unit ϵ_i of norm -1. From Kubota's work, we know the unit group of K has one of the two systems of fundamental units $\{\epsilon_1, \epsilon_2, \epsilon_3\}$ or $\left\{\epsilon_1, \epsilon_2, \sqrt{\epsilon_1\epsilon_2\epsilon_3}\right\}$. K has the former structure if and only if $\left[O_K^\times : \prod_{i=1}^3 O_{Q_i}^\times\right] = 1$ and K has no unit of norm -1; K has the latter structure if and only if $\left[O_K^\times : \prod_{i=1}^3 O_{Q_i}^\times\right] = 2$ and $z = \sqrt{\epsilon_1\epsilon_2\epsilon_3}$ is a unit in K of norm -1. We will show that a system of fundamental units for K is the latter structure, so K contains a unit z of norm -1.

Let h_i denote the class number of Q_i and let h denote the class number of K. Since $p, q \equiv 1 \mod 4$, genus theory tells us that h_1 and h_2 are odd, and in Kučera (1995) it is proven that $h_3 \equiv 2 \mod 4$. By Kuroda's class number formula for biquadratic fields, $h = 1/4 \cdot \left[O_K^\times : \prod_{i=1}^3 O_{Q_i}^\times\right] h_1 h_2 h_3 \in \mathbb{N}$, so it must be that $2 \left| \left[O_K^\times : \prod_{i=1}^3 O_{Q_i}^\times\right]\right.$. Thus the unit group of K must have system of fundamental units given by $\left\{\epsilon_1, \epsilon_2, \sqrt{\epsilon_1\epsilon_2\epsilon_3}\right\}$, implying that K contains a unit of norm -1.

□

Acknowledgments

This research was completed through the rise^3 undergraduate summer research program (now part of the Krulak Center) at Birmingham-Southern College in 2015 and 2016. We would like to thank the college for support to complete this project, including the Krulak Center, the Department of Mathematics, and the Department of Biology.

References

Artin, E. (1965). The Collected Papers of Emil Artin. Addison–Wesley Publishing Co., Inc., Reading, Mass.-London.

Fröhlich, A., & Taylor, M. J. (1991). Algebraic Number Theory (D. J. H. Garling, D. Gorenstein, T. T. Dieck, & P. Walters, Eds.). Cambridge University Press.

Gupta, R., & Murty, M. (1984). A remark on Artin's conjecture. Invent. Math., 1(78), 127-130.

Hooley, C. (1967). On Artin's conjecture. J. Reine Angew. Math., 225, 209–220.

Ireland, K., & Rosen, M. (1990). A classical introduction to modern number theory (Second ed.; S. Axler, F. W. Gehring, & K. A. Ribet, Eds.). Springer.

Kubota, T. (1956). Über den bizyklischen biquadratischen zahlkörper. Nagoya Math. J., 10, 65–85.

Kučera, R. (1995). On the parity of the class number of a biquadratic field. J. Number Theory, 52(1), 43–52. Retrieved from <ahref="http://dx.doi.org/10.1006/jnth.1995.1054"target="_blank">http://dx.doi.org/10.1006/jnth.1995.1054 doi: 10.1006/jnth.1995.1054

Kuroda, S. (1950). Über die klassenzahlen algebraischer zahlkörper. Nagoya Math. J., 1, 1–10.

Mollin, R. A., & Srinivasan, A. (2010). A note on the negative Pell equation. Int. J. Algebra, 4(17-20), 919–922.

Roskam, H. (2000). A quadratic analogue of Artin's conjecture on primitive roots. J. Number Theory, 81(1), 93–109.

Stadnik, M. E. (2017). A multiquadratic field generalization of Artin's conjecture. J. Number Theory, 170(1), 75–102.

Wada, H. (1966). On the class number and the unit group of certain algebraic number fields. J. Fac. Sci. Univ. Tokyo Sect. I, 13, 201–209.