The Mathematics Student ISSN: 0025-5742
Vol. 86, Nos. 1-2, January-June (2017), 39-50

NORM OR EXCEPTION?

KANNAPPAN SAMPATH AND B. SURY

(Received : 14 - 09 - 2016, Revised : 04 - 01 - 2017)

Abstract. In the study of class groups of real quadratic fields, one encounters norm form equations of the type $x^2 - dy^2 = k$. Apart from the usual approach from algebraic number theory, we discuss also how one uses methods from continued fractions. We demonstrate the methods through a particular example. The continued fraction method does not seem to be well-known apart from the basic theory used for the equations $x^2 - dy^2 = \pm 1$. This article could be useful to graduate students or researchers in number theory.

Introduction

In a first course on algebraic number theory, a typical homework problem may ask the student to determine the class group of a quadratic field. One is expected to determine the Minkowski constant and analyse the behaviour of the small primes not exceeding it. For instance, for $\mathbb{Q}(\sqrt{223})$, the primes up to 13 need to be considered. In this particular example, it is quite easily seen that 3 splits into the two prime ideals $P := (3, 1 + \sqrt{223})$ and $P' := (3, 1 - \sqrt{223})$, and that the ideal classes of prime ideals lying above the other primes are either trivial or, are equivalent to one of the primes P, P' dividing 3. Further, it is easy to show that P^3 is principal. The complete determination of the class group then boils down to checking whether there are elements of norm ± 3 in the ring of integers. Typically, when a solution is not easily visible, some congruence conditions rule out the existence of solutions. In the above example too, it is easy to see that

$$a^2 - 223b^2 = 3$$

has no integral solutions by looking at the equation modulo 4. However, it does not seem equally easy to prove that

$$a^2 - 223b^2 = -3$$

has no integral solutions. In this note, we look at this example and discuss two proofs. Both proofs have the potential to be applied more generally.

We discuss the first proof just for this example but, while giving the second proof, we take the opportunity to analyze the power of continued fractions. The employment of the continued fraction expansion of $\sqrt{d}$ (d positive non-square) to

2010 Mathematics Subject Classification: 11 D 57, 11 R 11
Keywords and Phrases: Norm equations; Continued fraction; Real quadratic fields.

determine the solutions of $x^2 - dy^2 = \pm 1$ is well-known. We point out that this amounts to looking for the units (equivalently, elements of norm ± 1, the norm being taken in quadratic field $\mathbb{Q}(\sqrt{d})$) in the ring $\mathbb{Z}[\sqrt{d}]$. But more generally, if we let ξ be an irrational real number satisfying a quadratic equation with coefficients in $\mathbb{Q}$ so that $\mathbb{Q}(\xi)$ is a real quadratic field (the so-called *real quadratic irrationalities*), then, the continued fraction of ξ can often be used to study the existence (or the lack thereof) of elements of $\mathbb{Z}[\xi]$ of "small" norm (as an element of $\mathbb{Q}(\xi)$) - see Theorem 2.10. It appears to us that these results are due to Lagrange and have been laid out carefully in Serret's seminal work on "higher" algebra [7, Chapitre II, Section I, §35, p.80]. In fact, at the time of writing this article, the only other text where we could find a discussion of this nature is the book [1] by Chrystal; here, one finds a thorough discussion of the less general Diophantine equation $x^2 - dy^2 = m$ for $m \neq \pm 1$. Chrystal alludes to the general case in Exercises XXXII, (52.); however, the formulation as it stands is incomplete and seems a little misleading. The underlying principle is that the elements of "*small*" norm, if there are any, must come from convergents of the continued fraction of ξ. The key point that is only implicit even in the references mentioned above, is the estimation of the number of convergents that we must compute before we can refute the existence of an element of a given "small" norm. Our exposition aims to make this very transparent (v. Lemma 2.13) while remaining short and self-contained.

The very general phenomenon outlined above does not seem so well-known; at any rate, this has not been expounded in most standard texts on algebraic number theory. After this article was written, we looked through recent texts and discovered a new book by Trifković ([8]) on algebraic number theory which also coincidentally discusses the very example above and we recommend this text to the reader interested in a more detailed study of the subject.

1. Class group of $\mathbb{Q}(\sqrt{223})$

Let us start with a more detailed discussion of the computation of the class group of the real quadratic field $k := \mathbb{Q}(\sqrt{223})$.

As $223 \equiv 3 \pmod 4$, we have $O_k = \mathbb{Z}[\sqrt{223}]$ and its discriminant equals 4×223. The Minkowski constant of k is $\sqrt{223}$. One looks at the splitting of the primes $2, 3, 5, 7, 11, 13$ in O_k. The prime 2 (as well as the prime 223) ramifies as it divides the discriminant; in fact,

$$2\mathbb{Z}[\sqrt{223}] = (2, 1 + \sqrt{223})^2$$

since the minimal polynomial $f = X^2 - 223$ becomes $X^2 - 1 = (X+1)^2$ mod 2. Also, f remains irreducible (equivalently, has no root) modulo 5, 7 or 13; so, these primes remain inert. Further, modulo 3, we have $X^2 - 223 = X^2 - 1 = (X+1)(X-1)$ which shows

$$3\mathbb{Z}[\sqrt{223}] = (3, 1 + \sqrt{223})(3, -1 + \sqrt{223}).$$

Modulo 11, $X^2 - 223 = X^2 - 3 = (X+5)(X-5)$ so that

$$11\mathbb{Z}[\sqrt{223}] = (11, 5+\sqrt{223})(11, -5+\sqrt{223}).$$

Now, if $(2, 1+\sqrt{223})$ is principal, it would be generated by an element of norm ± 2 because its square is $2\mathbb{Z}[\sqrt{223}]$ which has norm 4. It is easy locate an element of norm 2; viz., $15+\sqrt{223}$. It is then straightforward to check that

$$(2, 1+\sqrt{223}) = (15+\sqrt{223}).$$

Further, we can easily locate an element of norm $3 \times 11 = 33$, viz., $16+\sqrt{223}$. It is once again a straightforward task to check that

$$(3, 1+\sqrt{223})(11, 5+\sqrt{223}) = (16+\sqrt{223}).$$

Indeed, $16+\sqrt{223} = (1+\sqrt{223})(2(5+\sqrt{223}) - 11) - (3)(11)(13)$.

Now, let us find the order of $P = (3, 1+\sqrt{223})$.

As P has norm 3, we look for an element of norm ± 9 to ascertain whether P^2 is principal. Inspection of small values does not produce a solution. The next step is to look for an element of norm $\pm 3^3$ which would possibly generate P^3. Sure enough, the easily located element $14+\sqrt{223}$ of norm -27 satisfies

$$P^3 = (14+\sqrt{223}).$$

What is left is to ascertain whether P itself is principal; if it is not, the class group is the cyclic group of order 3 generated by the class of P. We shall prove that P is not principal. If P is principal, say $P = (a+b\sqrt{223})$, then

$$a^2 - 223b^2 = \pm 3.$$

Clearly, there is no solution with the positive sign on the right since the left hand side is $0, 1$ or 2 modulo 4. However, the proof of the fact that the equation has no solution with the negative sign on the right hand side, is not straightforward. We give two proofs. The first one is due to Peter Stevenhagen (personal correspondence); our main aim is to discuss the second proof at length. In both proofs, we do not need to separate the cases 3 and -3.

The fundamental unit of $\mathbb{Q}(\sqrt{223})$ is $\eta = 224 + 15\sqrt{223}$. This can be found simply by hand but while discussing the second proof, we give the details.

1.1. **First proof.** Let, if possible, $(3, 1+\sqrt{223}) = (x)$ for some $x \in \mathbb{Z}[\sqrt{223}]$. As $P^3 = (x^3) = (14 - sqrt223)$, we have

$$14 - \sqrt{223} = ux^3$$

for some unit u. Now, the fundamental unit

$$\eta = 224 + 15\sqrt{223} \equiv -1 \ mod \ 5 \ \mathbb{Z}[\sqrt{223}].$$

In particular, η becomes a cube in the finite field $F := \mathbb{Z}[\sqrt{223}]/5 \ \mathbb{Z}[\sqrt{223}]$ which has 5^2 elements. In particular, every unit (being a power of η) is a cube in this field. Hence, the image of $14 - \sqrt{223}$ is a cube. An element in the cyclic group F^* of order $5^2 - 1 = 24$ is a cube if, and only if, its 8-th power is 1. Let us compute the image of $(14 - \sqrt{223})^8$ in the field F:

$$\begin{aligned}(14-\sqrt{223})^8 = (-1-\sqrt{223})^8 \quad &= (1+223+2\sqrt{223})^4 = (-1+2\sqrt{223})^4\\ = (1+892-4\sqrt{223})^2 = (-2-4\sqrt{223})^2 \quad &= 4(1+2\sqrt{223})^2\\ = 4(1+892+4\sqrt{223}) \equiv 4(-2-\sqrt{223}) \quad &= 2+\sqrt{223}.\end{aligned}$$

But, $\sqrt{223}+2$ is not 1 in the cyclic group $(\mathbb{Z}[\sqrt{223}]/5\ \mathbb{Z}[\sqrt{223}])^*$. Otherwise, $223 = 1 \bmod 5\mathbb{Z}[\sqrt{223}]$ which is absurd as 222 is co-prime to 5. This completes the proof that P cannot be principal S

We deduce:

The ideal class group of $\mathbb{Q}(\sqrt{223})$ is cyclic, of order 3, generated by the class of $(3, 1+\sqrt{223})$. Further, the equation $a^2 - 223b^2 = -3$ has no integer solutions.

1.2. **A non-square.** Before embarking on the discussion on continued fractions required for the second proof, we make an interesting remark.

Rewriting the above equation as $a^2 + 3 = 223b^2$, one may argue within the field $\mathbb{Q}(\sqrt{-3})$ generated by the cube roots of unity. Its ring of integers is $\mathbb{Z}[\omega]$, a unique factorization domain where $\omega = \frac{-1+\sqrt{-3}}{2}$. If a is odd and b is even then $a^2 + 3 = 223b^2$ becomes equivalent to an equation

$$A^2 - A + 1 = 223B^2.$$

That is, $(A+\omega)(A+\omega^2) = 223B^2$.

Writing the element 223 is a product of two irreducible elements:

$$223 = (17+11\omega)(17+11\omega^2),$$

one has $A+\omega = (17+11\omega)(u+v\omega)$ or $A+\omega = (17+11\omega^2)(u+v\omega)$. Comparing the imaginary parts, one may deduce that there exists a number of the form $223s^2 + 79s + 7$ which is a perfect square. Therefore, we deduce:

Observation. *For an integer s, the number $223s^2 + 79s + 7$ cannot be a perfect square.*

In fact, write $223s^2 + 79s + 7 = t^2$. Then,

$$(446s + 79)^2 + 3 = 223(2t)^2.$$

This contradicts the fact that $a^2 - 223b^2 = -3$ has no solution.

It will be interesting to give a direct proof of the above observation.

2. Continued fractions and Small norms

2.1. **Continued fractions.** We recall the basic terminology of simple continued fractions relevant to our application to real quadratic fields. For a more elaborate discussion, we recommend the classical works [7, 2, 1, 3] and the recent text [8].

A *simple continued fraction* (S.C.F.) is an expression of the form

$$\lim_{n\to\infty}\left(a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\cdots\frac{1}{a_n}\right)$$

where $a_0 \in \mathbb{Z}$ and $\{a_n\}_{n>0}$ is a sequence of positive integers. In other words, an S.C.F. is the limit of the sequence whose nth term is

$$\ell_n := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots + \cfrac{1}{a_n}}}}. \tag{1}$$

One also writes the limit above as $a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\frac{1}{a_3+}\cdots$ or as $[a_0; a_1, a_2, \cdots]$ symbolically. Truncating this process at finite stages, the successive quotients

$$\frac{p_0}{q_0} := \frac{a_0}{1}, \frac{p_1}{q_1} := a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1}, \cdots$$

are called the *convergents* to the continued fraction. It can be proven by a straightforward induction that

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix}.$$

Immediately, a consideration of determinants gives:

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$$
$$p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$$

The most important fact about continued fractions that we need is the following observation due to Legendre [3]:

THEOREM 2.1. *If α is a real number which is irrational, and satisfies*

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{2s^2}$$

where $s > 0$, then r/s is a convergent to the continued fraction of α.

In algorithm 2.4 below, we study the algorithm for the S.C.F. for quadratic irrational to work out the small norms in the ring of integers of a real quadratic field. As a precursor to the general discussion, let us recall the classical facts about S.C.F. for $\sqrt{N}$ for positive square-free integers N.

2.2. **The S.C.F. of $\sqrt{N}$.** Let N be a square-free positive integer. The S.C.F. $\sqrt{N} = b_0 + \frac{1}{b_1+}\frac{1}{b_2+}\cdots$ is determined as

$$b_0 = a_1 = [\sqrt{N}], \qquad r_1 = N - a_1^2$$
$$b_1 = \left[\frac{\sqrt{N} + a_1}{r_1}\right], \qquad \text{etc.}$$

More generally, we have

$$b_n = \left[\frac{\sqrt{N} + a_n}{r_n}\right]$$

where $a_n = b_{n-1} r_{n-1} - a_{n-1}$ and $r_{n-1} r_n = N - a_n^2$. One shows easily that $a_{n+1}, r_{n+1} > 0$. Further, *if we know* that some r_k (say r_{n+1}) equals 1, then

$$(-1)^{n-1} = p_n^2 - Nq_n^2.$$

This is indeed the case (see [2]) and the key facts are summarized as:

LEMMA 2.2.

(i) *The b_n's recur.*
(ii) *The S.C.F. of $\sqrt{N}$ looks like $[b_0; \overline{b_1, b_2, \cdots, b_{n-1}, 2b_0}]$.*
(iii) *The penultimate convergent p_{n-1}/q_{n-1} before the recurring period gives a solution of $x^2 - Ny^2 = (-1)^n$.*

Hence, the penultimate convergent of the S.C.F. of $\sqrt{N}$ gives a solution of $x^2 - Ny^2 = \pm 1$ where the sign is positive or negative according as to whether the period is even or odd.

2.3. **The S.C.F. of real quadratic irrationalities.** Let us discuss how the above facts carry over from $\sqrt{N}$ to any element of a real quadratic field, which we christen a real quadratic irrationality.

DEFINITION 2.3. A number $\xi \in \mathbb{C} \setminus \mathbb{Q}$ is said to be a *real quadratic irrationality* if it satisfies an equation of the form $\xi^2 + p\xi + q = 0$ for uniquely determined rational numbers p and q satisfying $p^2 - 4q^2 > 0$.

Let ξ' denote the Galois conjugate of ξ (equal to $-p - \xi$ under the above notation). We have the following algorithm to produce the S.C.F. of a general real quadratic irrationality.

ALGORITHM 2.4. Let $\xi = \frac{P_0 + \sqrt{D}}{Q_0}$ be a real quadratic irrationality where D, P_0, Q_0 are positive integers. We assume, without loss of generality, that Q_0 divides $P_0^2 - D$ (otherwise, we may multiply P_0, Q_0 by Q_0 and D by Q_0^2).

Then, define the sequences $\{a_n\}_{n \geqslant 0}$, $\{\xi_n\}_{n \geqslant 0}$, $\{P_n\}_{n \geqslant 1}$ and $\{Q_n\}_{n \geqslant 1}$ of numbers by the following rule:

$$a_0 = [\xi_0] \qquad \text{and} \qquad \xi_1 = \frac{1}{\xi_0 - a_0} = \frac{P_1 + \sqrt{D}}{Q_1}$$

$$a_1 = [\xi_1] \qquad \text{and} \qquad \xi_2 = \frac{1}{\xi_1 - a_1} = \frac{P_2 + \sqrt{D}}{Q_2}$$

In general,

$$a_{m-1} = [\xi_{m-1}] \text{ and } \xi_m = \frac{1}{\xi_{m-1} - a_{m-1}} = \frac{P_m + \sqrt{D}}{Q_m}.$$

Then, $\xi = [a_0; a_1, a_2, \cdots]$ is the S.C.F. of ξ.

The following observations on this algorithm are the most useful ones:

LEMMA 2.5. *Let $\{p_n/q_n\}$ be the sequence of convergents of a quadratic irrational ξ. With notations as above, all P_i, Q_i are integers and, the following equations hold:*

$$\xi = (a_0; a_1, \dots, a_{n-1}, \xi_n)\,, \quad n \geqslant 1; \tag{2}$$

$$P_{n+1} = a_n Q_n - P_n, \quad n \geqslant 0 \tag{3}$$

$$P_{n+1}^2 + Q_n Q_{n+1} = D, \quad n \geqslant 0 \tag{4}$$

$$Q_{n+1} = Q_{n-1} + Q_n(P_n - P_{n+1}) \tag{5}$$

$$(-1)^n Q_n / Q_0 = (p_{n-1} - \xi q_{n-1})(p_{n-1} - \xi' q_{n-1}) \tag{6}$$

It is the last equation that is the protagonist of this story: it tells us that $p_{n-1} - q_{n-1}\xi$ solves the norm-form equation $N(\mathfrak{z}) = (-1)^n Q_n/Q_0$ where $N(\cdot)$ stands for the norm on the quadratic field $\mathbb{Q}(\xi)$. We shall soon discover that with appropriate bound on H, a primitive solution (if it exists at all) to the norm form equation $N(\mathfrak{z}) = H$ with $\mathfrak{z} \in \mathbb{Z}[\xi]$ must arise from convergents (see Theorem 2.10).

Proof. We prove the equalities asserted in the lemma, from which it follows inductively that the P_i's and the Q_i's are integers. The first equality holds by definition. The next two equalities are consequences of the identity:

$$\frac{P_{n+1} + \sqrt{D}}{Q_{n+1}} = \frac{1}{\frac{P_n + \sqrt{D}}{Q_n} - a_n}.$$

Indeed, multiply out and equate rational and irrational parts.
To prove the penultimate equality, note that

$$Q_n Q_{n+1} = D - P_{n+1}^2 = D - (a_n Q_n - P_n)^2 = P_n^2 + Q_{n-1} Q_n - (a_n Q_n - P_n)^2$$

which gives $Q_{n+1} = Q_{n-1} + a_n(P_n - P_{n+1})$.
Finally, we prove that the last equality follows from certain properties of convergents as follows. We know that the complete quotients ξ_n give us

$$\frac{P_0 + \sqrt{D}}{Q_0} = \frac{p_{n-1}\xi_n + p_{n-2}}{q_{n-1}\xi_n + q_{n-2}}.$$

Using the expression $\xi_n = \frac{P_n + \sqrt{D}}{Q_n}$, we have

$$\frac{P_0 + \sqrt{D}}{Q_0} = \frac{p_{n-1} P_n + p_{n-2} Q_n + p_{n-1}\sqrt{D}}{q_{n-1} P_n + q_{n-2} Q_n + q_{n-1}\sqrt{D}}.$$

A comparison of rational and irrational parts gives us:

$$q_{n-1} P_n + q_{n-2} Q_n = Q_0 p_{n-1} - P_0 q_{n-1};$$

$$p_{n-1} P_n + p_{n-2} Q_n = P_0 p_{n-1} + \left(\frac{D - P_0^2}{Q_0}\right) q_{n-1}.$$

Using $p_{n-1} q_{n-2} - p_{n-2} q_{n-1} = (-1)^n$, we obtain

$$(-1)^n P_n = P_0 (p_{n-1} q_{n-2} + p_{n-2} q_{n-1}) + \left(\frac{D - P_0^2}{Q_0}\right) q_{n-1} q_{n-2} - Q_0 p_{n-1} p_{n-2};$$

$$(-1)^n Q_n = -2 p_{n-1} q_{n-1} P_0 + \left(\frac{P_0^2 - D}{Q_0}\right) q_{n-1}^2 + Q_0 p_{n-1}^2.$$

As $\xi + \xi' = \frac{2P_0}{Q_0}$, $\xi\xi' = \frac{P_0^2 - D}{Q_0^2}$, we obtain $N(p_{n-1} - \xi q_{n-1}) = (-1)^n Q_n / Q_0$. □

The key periodicity feature of this algorithm is given in the following theorem (see Chrystal, Chapter XXXIII, §4):

THEOREM 2.6 (Euler-Lagrange). *The sequence $(a_n)_{n\geqslant 0}$ in the continued fraction of the quadratic irrationality ξ is eventually periodic; that is, there are positive integers t and h such that $a_{n+h} = a_n$ for all $n \geqslant t$ and h is the least positive integer such that $a_{n+h} = a_n$ for all sufficiently large n and t is the least positive integer such that $a_{t+h} = a_t$.*

It is evident that the integers h and t with properties in Theorem 2.6 are uniquely determined. The word $a_0 \dots a_{t-1}$ is called the *preperiod* and, the number t is called the *length of the preperiod* of the sequence $(a_n)_n$. The number h is called the *length of the period* of $(a_n)_n$ and is denoted by $\ell(\xi)$. A convenient shorthand for this situation is the following notation:

$$(a_n)_n := (a_0, \dots, a_{t-1}, \overline{a_t, \dots, a_{t+h-1}}).$$

For our purposes, it is necessary to be able to compute the length of the preperiod of quadratic irrationals. The proof we present is the one of the key parts of the proof of the periodicity theorem above and consequently the theorem itself is known but is seldom formulated this way:

THEOREM 2.7. *The following are equal for a quadratic irrational ξ:*

(1) The length of the preperiod of ξ.
(2) The least index t such that $\xi_t > 1$ and $-1 < \xi_t' < 0$.
(3) The least index t such that $0 < P_t < \sqrt{D}$ and $0 < Q_t < P_t + \sqrt{D}$.

Proof. It is clear that the numbers defined in (2) and (3) are equal. Let k be the preperiod of ξ. Then, it follows from the uniqueness theorem that $\xi_k = (\overline{a_k, \dots, a_{k+h-1}})$. Therefore, we have

$$\xi_k = (a_k, \dots, a_{k+h-1}, \xi_k). \tag{7}$$

Notice that $\xi_k > a_k = a_{k+h} \geqslant 1$. Moreover, (7) gives us a quadratic equation satisfied by ξ_k (and hence ξ_k'):

$$F(\xi_k) = q_{k+h-1}\xi_k^2 + (q_{k+h-2} - p_{k+h-1})\xi_k - p_{k+h-2} = 0.$$

Note now that $F(0) = -p_{k+h-2} < 0$ and $F(-1) = q_{k+h-1} + p_{k+h-1} - q_{k+h-2} - p_{k+h-2} > 0$ since the numerator and denominator of a convergent form a (strictly) increasing sequence. Therefore F has a root in $(-1, 0)$ which proves that $-1 < -\xi_k' < 0$. Thus, we have that $k \geqslant t$.
If $k > t$, we shall conclude that $a_{k-1} = a_{k+h-1}$ which will contradict the definition of preperiod. We use the following lemma which easily follows by induction.

LEMMA 2.8. *If ξ_t satisfies the conditions $\xi_t > 1$ and $-1 < \xi_t' < 0$, then, so does ξ_n for all $n \geqslant t$.*

The theorem follows from above as $a_n = [-1/\xi'_{n+1}]$ for all $n \geqslant t$ and, in particular, we have that $a_{k-1} = a_{k+h-1}$ taking $n = k-1$. □

Now we have the following corollary.

Corollary 2.9. *Let $D > 0$ be a square-free integer. The length of the preperiod of $\sqrt{D}$ and that of $\frac{-1+\sqrt{D}}{2}$ are both 1.*

Proof. Let $a_0 = [\xi]$ where ξ is one of the quadratic irrationalities in the statement. Then

$$P_1 = \begin{cases} a_0, & \text{if } \xi = \sqrt{D} \\ 2a_0+1, & \text{if } \xi = \frac{-1+\sqrt{D}}{2} \end{cases} \quad \text{and} \quad Q_1 = \begin{cases} D - a_0^2, & \text{if } \xi = \sqrt{D} \\ \frac{D-(2a_0+1)^2}{2}, & \text{if } \xi = \frac{-1+\sqrt{D}}{2} \end{cases}$$

It is now easily verified that the least index for which inequalities in (3) of the above theorem hold in each case is $t = 1$. □

2.4. **Small norms.** The existence of elements of norm H (where H is an integer) in $\mathbb{Z}[\xi]$ is equivalent to the existence of an integral solution to the equation

$$(X + \xi Y)(X + \xi' Y) = H. \tag{8}$$

Note first that if $x, y \in \mathbf{Z}$ are integers satisfying $(x + \xi y)(x + \xi' y) = H$, we may replace H by $H/(x,y)^2$, and obtain a new solution $X = x/(x,y), Y = y/(x,y)$ to (8), which are relatively prime. An integral solution to (8) with $(x,y) = 1$ is said to be primitive.

The key result which is relevant to our original problem is the following observation that primitive solutions come from convergents of ξ when ξ generates the ring of integers in a real quadratic field K:

Theorem 2.10. *Let ξ be a real, quadratic irrational written in the form*

$$\xi = \frac{P + \sqrt{D}}{Q}.$$

Suppose that $\xi > 0 > \xi'$ (equivalently $Q > 0$ and $-\sqrt{D} < P < \sqrt{D}$). If x, y are relatively prime integers such that $(x + \xi y)(x + \xi' y) = H$ with $|H| < \frac{\xi - \xi'}{2} = \frac{\sqrt{D}}{Q}$, then x/y is a convergent to $-\xi'$.
Moreover, we need to look at only the first lcm $(2, \ell(\xi)) + 1$ convergents.

Proof. Suppose first that $H > 0$. Thus $x + \xi' y > 0$ and so $x + \xi y > (\xi - \xi')y$. So, we have

$$0 < x + \xi' y < \frac{H}{(\xi - \xi')y} < \frac{1}{2y}$$

from which it follows that x/y is a convergent to $-\xi'$.

Now, if $H < 0$, we then have that $x + y\xi' < 0$ so that we have

$$0 < y + \frac{x}{\xi'} = \frac{H}{\xi'(x + y\xi)} = \frac{-H}{-\xi'(x + y\xi)} < \frac{\xi - \xi'}{2(-\xi')(x + y\xi)} < \frac{1}{2x}$$

where the last inequality amounts to checking that

$$x(\xi - \xi') < (-\xi')(x + y\xi)$$

which holds since $\xi > 0$ and $x + y\xi' < 0$. This shows that y/x is a convergent of $-\xi'^{-1}$. But we note that if x has the S.C.F. $[a_0; a_1, a_2, \dots]$, then, x^{-1} has the S.C.F. $[0; a_0, a_1, \dots]$ if $a_0 > 0$ and $[a_1; a_2 \dots]$ if $a_0 = 0$. Therefore, every non-zero convergent of x is also a convergent of x^{-1}. Thus, we have that x/y is a convergent of $-\xi'$. We defer the proof of the last assertion to Lemma 2.13. □

The above theorem immediately yields the following corollary.

Corollary 2.11. *Let D be a square-free positive integer, let K denote the quadratic field $\mathbb{Q}(\sqrt{D})$, let d_K be its discriminant:*

$$d_K = \begin{cases} 4D, & \text{if } D \equiv 2, 3 \bmod 4 \\ D, & \text{if } D \equiv 1 \bmod 4 \end{cases} \tag{9}$$

Let ω_D denote the quadratic irrationality

$$\omega_D = \begin{cases} \sqrt{D}, & D \equiv 2, 3 \bmod 4 \\ \frac{-1+\sqrt{D}}{2}, & D \equiv 1 \bmod 4 \end{cases} \tag{10}$$

so that $\mathcal{O}_K = \mathbb{Z}[\omega_D]$. Suppose that $|H| < \frac{\sqrt{d_K}}{2}$. The primitive elements of norm H in K come from convergents of ω_D.

Here, it is important that we view $\mathcal{O}_K$ as $\mathbb{Z}$-module with respect to the basis $\{1, -\omega'_D\}$ as is customary.

Remark 2.12. Note that the bound on H is reminiscent of Gauss's bound; that is, in any ideal class in a quadratic field K, there is an integral ideal whose norm is atmost $\frac{\sqrt{d_K}}{2}$.

To make this principle practical, one needs a bound on the number of convergents one has to compute. This is given in the following lemma.

Lemma 2.13. *The fundamental primitive solutions of* (8)*, if they exist, are to be found among the first $\ell' + 1$ convergents where $\ell' = lcm(2, \ell(\xi))$.*

Proof. The key ingredient in the proof is Theorem 2.15 which discusses the induced periodicity in the sequence $((-1)^n Q_n)_n$. Let us first reduce this question to the periodicity of (Q_n). This is a consequence of the following simple lemma:

Lemma 2.14. *Let $(u_n)_{n \geqslant 0}$ be an eventually periodic sequence with preperiod of length t and period h; further suppose that $u_n \neq 0$ for all $n \geqslant t$. Then, the sequence $(v_n := (-1)^n u_n)_{n \geqslant 0}$ is eventually periodic with preperiod of length t and period of length h' where h' is a divisor of $lcm(2, h)$.*
Furthermore, if h is odd, then, $h' = 2h$.

Now, we may summarize the above discussion in the theorem.

Theorem 2.15. *Let ξ be a quadratic irrational. Let $(a_n)_{n \geqslant 0}$ be its continued fraction expansion. Then*

(i) *The sequence (a_n) is eventually periodic.*
(ii) *The sequence (ξ_n) is eventually periodic.*

(iii) *The sequence* (Q_n) *is eventually periodic.*

(iv) *The preperiod and period of the above sequences are all equal.*

Proof. (i) is precisely Theorem 2.6. (ii) (and hence (iii) and (iv)) follows by noting that for any integer $n \geqslant 0$, we have $\xi_n = (a_k)_{k \geqslant n}$ by Lemma 2.5. □

These observations now complete the proof of our theorem. □

3. Examples

We illustrate the results of the last section by showing that $\mathbb{Z}[\sqrt{223}]$ has no elements of norm -3.

Example 3.1. It is straightforward to verify that $\sqrt{223} = [14; \overline{1, 13, 1, 28}]$. Here is the full computation: we begin by noting that $14 < \sqrt{223} < 15$ so

$$\begin{aligned}
\sqrt{223} = 14 + \sqrt{223} - 14 = 14 + {} & \frac{1}{\frac{\sqrt{223}+14}{27}} \\
= 14 + {} & \frac{1}{1+}\frac{1}{\frac{\sqrt{223}+13}{2}} \\
= 14 + {} & \frac{1}{1+}\frac{1}{13+}\frac{1}{\frac{\sqrt{223}+13}{27}} \\
= 14 + {} & \frac{1}{1+}\frac{1}{13+}\frac{1}{1+}\frac{1}{\sqrt{223}+14} \\
= 14 + {} & \frac{1}{1+}\frac{1}{13+}\frac{1}{1+}\frac{1}{28+}\frac{1}{\frac{\sqrt{223}+14}{27}} \quad = \quad [14; \overline{1, 13, 1, 28}].
\end{aligned}$$

The convergents are easily computed to be

$$\frac{p_0}{q_0} = \frac{14}{1} \qquad \frac{p_1}{q_1} = \frac{15}{1}$$

$$\frac{p_2}{q_2} = \frac{209}{14} \qquad \frac{p_3}{q_3} = \frac{224}{15}$$

and we have (cf. Lemma 2.5 (6))

$$14^2 - 223 = -27; \qquad 15^2 - 223 = 2;$$

$$209^2 - 223 \cdot 14^2 = -27; \qquad 224^2 - 223 \cdot 15^2 = 1.$$

This shows that there are no elements of norm -3 in $\mathbb{Z}[\sqrt{223}]$. More precisely, we see that the set of norms H in $\mathbb{Z}[\sqrt{223}]$ with $|H| \leqslant 14$ is $\{1, 2, 4, 8\}$.

To illustrate the differences that occur in the case $D \equiv 1 \bmod 4$, let us study the small norms in $\mathbb{Q}(\sqrt{229})$.

Example 3.2. Let $K = \mathbb{Q}(\sqrt{229})$. From Corollary 2.11 and Lemma 2.13, we must work out the first few convergents of S.C.F. of $\omega := \omega_{229} = \frac{-1+\sqrt{229}}{2}$ to find the list of all norms H with $|H| < 8$ in $\mathcal{O}_K$. Recall that $\{1, \xi\}$ where $\xi = -\omega'$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$.

We compute the S.C. F. of ω:

$$\omega = 7 + \frac{\sqrt{229} - 15}{2} = 7 + \frac{1}{\frac{\sqrt{229}+15}{2}} = 7 + \frac{1}{15 + \frac{\sqrt{229}-15}{2}} \text{ etc.,} = 7 + \frac{1}{15+}\frac{1}{15+}\frac{1}{15+}\cdots$$

By Lemma 2.13, we must work out the first 3 convergents. These are easily computed to be

$$\frac{p_0}{q_0} = \frac{7}{1}, \frac{p_1}{q_1} = \frac{106}{15}, \frac{p_2}{q_2} = \frac{1597}{226}.$$

From here, we have the following (cf. Lemma 2.5 (6)):

$$N(p_0 + \xi q_0) = -1, \quad N(p_1 + \xi q_1) = 1, \quad N(p_2 + \xi q_2) = -1.$$

Thus, we see that the only norms H with $|H| < 8$ are $\{\pm 1, \pm 4\}$. In particular, there are no elements of norm $\pm 2, \pm 3, \pm 5, \pm 6, \pm 7$.

While ± 2 and ± 7 are non-squares mod 229, one checks that ± 3 and ± 5 are squares mod 229; in particular, there are no obvious local obstructions for the norm form to represent these primes.

Acknowledgment. We would like to thank the referee for carefully going through the article.

References

[1] Chrystal, G., *Algebra: An Elementary Text-Book*, Volume II, 2nd Edition, Adam and Charles Black, London, England, 1900.

[2] Hall, H. S. and Knight, S. R., *Higher Algebra*, 4th Edition, Macmillan and Co., London, England, 1891.

[3] Hardy, G. H. and Wright, E. M., *Theory of Numbers*, Oxford, Clarendon, 1938.

[4] Lagrange, J. L., Additions au mémoire sur la ré solution des équations numériques, *Mém. Acad. Royale Sc. et belles-lettres*, Berlin, **24**, 1770 (= Œuvres II, 581–652).

[5] Matthews, K., The Diophantine equation $ax^2 + bx + cy^2 = N$, $D = b^2 - 4ac > 0$, *J. Théor. Nombres Bordeaux*, **14**(1): 257–270, 2002.

[6] Pavone, M., A Remark on a Theorem of Serret, *J. Number Theory*, **23**, 268–278, 1986.

[7] Serret, J. A., *Cours D'algébre Supérieure*, Tome Premier, Gauthier-Villars, Paris, 1877.

[8] Trifković, M., *Algebraic theory of quadratic numbers*, Springer-Verlag, New York, 2013.

Kannappan Sampath
Department of Mathematics, University of Michigan
Ann Arbor, Michigan 48105, USA
knsam@umich.edu

B. Sury
Statistics and Mathematics Unit
Indian Statistical Institute
8th Mile Mysore Road, Bangalore-560059, India
sury@ms.isibang.ac.in