International Journal of Number Theory

On Monic Binary Quadratic Forms

Vadim Ponomarenko
Department of Mathematics and Statistics, San Diego State University, 5500 Campanile Drive, San Diego California USA
vponomarenko@mail.sdsu.edu

We consider the quadratic form $x^2 + mxy + ny^2$, where $|m^2 - 4n|$ is prime. Under the assumption that a particular, small, finite set of integers is representable, we determine all integers representable by this form.

Keywords: Binary quadratic form; Law of quadratic reciprocity; prime number.

Mathematics Subject Classification 2010: 11E16, 11D72, 11D41

1. Foreword

Reader, beware! This manuscript was produced as an extension of [1]. However, it appears that its contents are known already. A reviewer wrote: "The results follow from classical results combining Minkowski's class group bound from the geometry of numbers with Gauss relation between binary quadratic forms and quadratic number fields."

One further comment: by an appropriate substitution $x \to x + ky$, we may assume that form $f(x, y) = x^2 + mxy + ny^2$ has $m = 1$. That is, without loss we may consider only the form $f(x, y) = x^2+xy+ny^2$. This fact was observed after the manuscript was decisively rejected, so it seemed pointless to update the manuscript.

2. Introduction

Representation of integers by quadratic forms is a classical problem, with major contributions by Fermat, Euler, Lagrange, and Gauss. We consider those forms that are binary, quadratic, monic, and with a cross term. Specifically, given $m, n \in \mathbb{Z}$ with associated monic quadratic form $f(x, y) = x^2 + mxy + ny^2$, we define $\tau = \tau(m, n) = |m^2 - 4n|$, the absolute value of the discriminant of this form. We will study τ to determine which integers $f(x, y)$ represents.

Recently in [3], the form $\tau(1, 1) = 3$ was fully analyzed. More recently in [1], the primes represented by forms $\tau(1, 1) = 3$ and $\tau(1, -1) = 5$ were determined. We extend these results to all forms with prime τ, provided Condition P holds (as defined below). We have verified condition P, computationally, for $\tau = 3, 5, 7, 11, 13, 17, 19, 23, 29, 37, 41, 43, 53, 61, 67, 101, 163, 173, 197$. It likely holds

for other τ as well, as only $\tau < 200$ were tested. It appears that $\tau = 31$ is the first prime for which Condition P fails.

Our results are restricted to τ prime. Note that if τ is prime, then m must be odd, and hence τ is also odd. We classify τ into cases via the following.

Definition 2.1. *Let $\tau \in \mathbb{N}$ be an odd prime. We say that τ is of Type I if $\tau \equiv 3 \pmod 4$; we say that τ is of Type II if $\tau \equiv 1 \pmod 4$.*

Note that, by some simple case analysis, if $\tau = 4n - m^2$ (i.e. $4n > m^2$), then τ is of Type I. If, instead, $\tau = m^2 - 4n$ (i.e. $m^2 > 4n$), then τ is of type II. The set of representable integers is a monoid under multiplication.

Lemma 2.2 (from [1]). *Let $m, n \in \mathbb{Z}$ and set $\mathfrak{K}_{m,n} = \{x^2+mxy+ny^2 : x, y \in \mathbb{Z}\}$, the set of representable integers. Then $(\mathfrak{K}_{m,n}, \times)$ is a monoid.*

Proof. Closure follows from the observation that $(a^2+mab+nb^2)(c^2+mcd+nd^2) = (ac-nbd)^2+m(ac-nbd)(bc+ad+mbd)+n(bc+ad+mbd)^2$. Identity follows from $1 = 1^2 + m(1)(0) + n(0)^2$. □

We now define $\mathfrak{K}'_{m,n} = \{x^2 + mxy + ny^2 : x, y \in \mathbb{Z}, \gcd(x, y) = 1\}$, a subset of $\mathfrak{K}_{m,n}$. Note that all nonzero squarefree elements of $\mathfrak{K}_{m,n}$ are in $\mathfrak{K}'_{m,n}$ (in particular, all primes). We call $\mathfrak{K}_{m,n}$ of type I/II, based on whether $\tau = |m^2 - 4n|$ is of type I/II. Note that the type of $\mathfrak{K}_{m,n}$ is determined solely by τ, independently of choice of m, n. For example, $5 = \tau(1, -1) = \tau(3, 1)$. Theorem 4.8 will prove that $\mathfrak{K}_{m,n}$ depends only on τ and Condition P, to be defined below (hence $\mathfrak{K}_{1,-1} = \mathfrak{K}_{3,1}$).

Let τ be an odd prime. We define the set $\mathfrak{P}_\tau$ as follows, using Legendre symbols (for this and other standard notation, see [2]).

$$\mathfrak{P}_\tau = \begin{cases} \{p \text{ prime} : p \le \sqrt{\frac{\tau}{3}}, \left(\frac{p}{\tau}\right) = 1\} & \tau \text{ is of Type I} \\ \{p \text{ prime} : p \le \sqrt{\frac{\tau}{3}}, \left(\frac{p}{\tau}\right) = 1\} \cup \{-1, \tau\} & \tau \text{ is of Type II.} \end{cases}$$

Note that $\mathfrak{P}_\tau$ is a finite set of integers, all prime (except perhaps -1). Most of our results require the following condition. It states that all elements of $\mathfrak{P}_\tau$ must be representable.

$$\mathfrak{P}_\tau \subseteq \mathfrak{K}_{m,n} \qquad \text{(Condition P)}$$

We determine all representable primes (in Theorems 3.1 and 4.6). We then find all representable integers (in Theorem 4.8). A prime turns out to be representable if and only if it is a quadratic residue modulo τ; a positive integer turns out to be representable if and only if each quadratic nonresidue prime in its factorization appears to an even power.

Computational evidence suggests that our results hold when τ is not prime. However we have been unable to remove either this restriction, or Condition P.

3. Preliminaries

Our first result proves non-representability for roughly half of $\mathbb{Z}$. If $t \in \mathbb{Z}$ is a quadratic nonresidue, then it is not representable. Theorem 3.1 does not require Condition P. Theorems 4.6 and 4.8 provide a converse to Theorem 3.1; both require Condition P.

Theorem 3.1. *Let $m, n, t \in \mathbb{Z}$ with $\tau = |m^2 - 4n|$ prime and $\tau \nmid t$. Suppose that t is a quadratic nonresidue modulo τ. Then $t \notin \mathfrak{K}_{m,n}$.*

Proof. We assume by way of contradiction the existence of $a, b \in \mathbb{Z}$ with $t = a^2 + mab + nb^2$. Multiplying by 4 and working modulo τ, we have $4t \equiv 4a^2 + 4mab + 4nb^2 \equiv (2a+mb)^2 + b^2(4n-m^2) \equiv (2a+mb)^2$. Hence $1 = \left(\frac{4t}{\tau}\right) = \left(\frac{t}{\tau}\right)\left(\frac{2}{\tau}\right)^2 = \left(\frac{t}{\tau}\right) = -1$, a contradiction. □

We next consider the special case of representing prime τ itself. If τ is of Type I, then τ can always be represented as $f(-m, 2) = (-m)^2 + m(-m)2 + 4n = -m^2 + 4n = \tau$. If τ is of Type II, there is no such nice formula. For example, $37 = \tau(1, -9) \in \mathfrak{K}_{1,-9}$ as $37 = f(31, 12)$. For the slightly larger prime $97 = \tau(11, 6) \in \mathfrak{K}_{11,6}$ as $97 = f(-116837, 11208)$. Condition P allows us to avoid this difficulty by assuming that τ is represented.

We now consider the case of representing -1. By Fermat's theorem on the sum of two squares, those τ of Type II can be written as the sum of two squares. If one of those squares is 1^2 or 2^2, then -1 will be representable by Lemma 3.2. Otherwise, we avoid this difficulty by imposing Condition P. The smallest prime of type II for which Lemma 3.2 doesn't apply is $41 = 4^2 + 5^2$.

Lemma 3.2. *Let $m, n \in \mathbb{Z}$ with $\tau = m^2 - 4n$ prime of type II. If there is some $k \in \mathbb{Z}$ with $\tau = 1 + k^2$ or $\tau = 4 + k^2$, then $-1 \in \mathfrak{K}_{m,n}$.*

Proof. If $\tau = 1 + k^2$, we have $f(-m-k, 2) = (-m-k)^2 + m(-m-k)2 + 4n = k^2 - (m^2 - 4n) = -1$. If $\tau = 4 + k^2$, we first note that m, k are both odd. Then, we calculate $f(\frac{-m-k}{2}, 1) = \frac{1}{4}(k^2 - m^2 + 4n) = -1$. □

Lemma 3.3 gives a condition for a monoid of type II to be nicely symmetric around 0. That condition is always met if Condition P holds.

Lemma 3.3. *Let $m, n \in \mathbb{Z}$ with $\tau = m^2 - 4n$ prime of type II. Suppose that $-1 \in \mathfrak{K}_{m,n}$. Then, for every $t \in \mathbb{Z}$, $t \in \mathfrak{K}_{m,n}$ if and only if $-t \in \mathfrak{K}_{m,n}$.*

Proof. Apply Lemma 2.2 to $t = (-1)(-t)$ and $-t = (-1)(t)$. □

If, instead, the monoid is of type I, then it contains no negative integers at all.

Lemma 3.4. *Let $m, n \in \mathbb{Z}$ with $\tau = 4n - m^2$ prime of type I. Then $\mathfrak{K}_{m,n} \subseteq \mathbb{N}_0$.*

Proof. Let $a, b \in \mathbb{Z}$. Since $4n > m^2$, we must have $n > 0$. Set $s = \frac{m}{\sqrt{n}}$, and $c = b\sqrt{n}$. We have $a^2 + mab + nb^2 = a^2 + sac + c^2 = \frac{2+s}{4}(a+c)^2 + \frac{2-s}{4}(a-c)^2$. Since $4n > m^2$, $|s| < 2$ and hence both $\frac{2+s}{4}$ and $\frac{2-s}{4}$ are positive. Thus $a^2 + mab + nb^2 \geq 0$, with equality only for $a = b = 0$. □

4. Representing Quadratic Residues

We turn now to the question of representing quadratic residues. This is harder than Theorem 3.1, as not all quadratic residues are representable. First, in several steps we prove Theorem 4.6, which resolves representation of primes that are quadratic residues. Then, we prove Theorem 4.8, which resolves representation of all integers.

This next lemma, relying on the law of quadratic reciprocity, is the starting point toward Theorem 4.6. It will be needed for all primes except $2, \tau$.

Lemma 4.1. *Let $m, n \in \mathbb{Z}$ with $\tau = |m^2 - 4n|$ prime. Let p be any odd prime different from τ. Then p is a quadratic residue modulo τ, if and only if $m^2 - 4n$ is a quadratic residue modulo p.*

Proof. Suppose first that $m^2 - 4n > 0$. By quadratic reciprocity, $1 = \left(\frac{m^2-4n}{p}\right)\left(\frac{p}{m^2-4n}\right)$, since $m^2 - 4n \equiv m^2 \equiv 1 \pmod 4$. On the other hand, if $m^2 - 4n < 0$, then $(-1)^{(p-1)/2} = \left(\frac{\tau}{p}\right)\left(\frac{p}{\tau}\right)$, since $\tau \equiv -(m^2 - 4n) \equiv -1 \pmod 4$. But also $\left(\frac{\tau}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{m^2-4n}{p}\right) = (-1)^{(p-1)/2}\left(\frac{m^2-4n}{p}\right)$. In both cases, $1 = \left(\frac{m^2-4n}{p}\right)\left(\frac{p}{\tau}\right)$. □

Our approach to prove that some $p \in \mathfrak{K}_{m,n}$ will be to start with $pt \in \mathfrak{K}_{m,n}$ for some integer t. The following strong lemma shows that if p is a nonresidue modulo τ, then not only is p not in $\mathfrak{K}'_{m,n}$, but no multiple of p is in $\mathfrak{K}'_{m,n}$ either. It also gives examples of nonrepresentible quadratic residues. If p, q are distinct, prime, nonresidues, then $pq \notin \mathfrak{K}'_{m,n}$. A simple argument then shows that $pq \notin \mathfrak{K}_{m,n}$, even though pq is a quadratic residue.

Lemma 4.2. *Let $m, n \in \mathbb{Z}$ with $\tau = |m^2 - 4n|$ prime. Let p be any odd prime different from τ and let $t \in \mathbb{Z}$. If p is a quadratic nonresidue modulo τ, then $pt \notin \mathfrak{K}'_{m,n}$.*

Proof. We assume by way of contradiction the existence of $a, b \in \mathbb{Z}$ with $pt = a^2 + mab + nb^2$ and $\gcd(a, b) = 1$. If $p|b$, then $p|(pt - mab - nb^2)$, so $p|a$, which contradicts $\gcd(a, b) = 1$. Hence $p \nmid b$, and we can choose an integer c so that $cb \equiv 1 \pmod p$. Working modulo p, we have $0 \equiv a^2 + mab + nb^2 \equiv b^2((ac)^2 + m(ac) + n)$. Hence $0 \equiv 4((ac)^2 + m(ac) + n) \equiv (2ac + m)^2 + 4n - m^2$, and thus $(2ac + m)^2 \equiv m^2 - 4n \pmod p$. Thus $m^2 - 4n$ is a quadratic residue, modulo p. By Lemma 4.1, p is a quadratic residue modulo τ; this contradicts hypothesis. □

Since every odd prime τ has quadratic nonresidues, we can apply Dirichlet's theorem on arithmetic progressions to find some odd prime $p \neq \tau$ that is a quadratic

nonresidue modulo τ. Applying Lemma 4.2 to this p and to $t = 0$, implies that $0 \notin \mathfrak{K}'_{m,n}$.

We now present an analogue of Lemma 4.2 for $p = 2$.

Lemma 4.3. *Let $m, n, t \in \mathbb{Z}$ with $\tau = |m^2 - 4n|$ prime. If 2 is a quadratic nonresidue modulo τ, then $4t \notin \mathfrak{K}'_{m,n}$.*

Proof. Since $\left(\frac{2}{\tau}\right) = -1$, by the second supplement to the law of quadratic reciprocity, we must have $m^2 - 4n = \pm\tau \equiv \pm 3 \pmod 8$. A simple case analysis shows that m, n are both odd. Assume now by way of contradiction the existence of $a, b \in \mathbb{Z}$ with $4t = a^2 + mab + nb^2$ and $\gcd(a, b) = 1$. In particular, a, b cannot both be even. If a, b are both odd, then $a^2 + mab + nb^2$ is also odd, a contradiction. If b is odd and $a = 2k$ is even, we have $0 \equiv (2k)^2 + m(2k)b + nb^2 \equiv b(2mk + nb) \pmod 4$. But now $4|(2mk + nb)$, so nb is even and hence b is even, a contradiction. Lastly, if a is odd and $b = 2j$ is even, we have $0 \equiv a^2 + ma(2j) + n(2j)^2 \equiv a(a + 2mj) \pmod 4$. But now $4|(a + 2mj)$, so a is even, a contradiction. □

We now represent, not yet an arbitrary prime, but some integer multiple thereof. The condition $p > \sqrt{\frac{\tau}{3}}$ is why most of Condition P is imposed. An improvement here would equally improve Condition P.

Lemma 4.4. *Let $m, n \in \mathbb{Z}$ with $\tau = |m^2 - 4n|$ prime. Let p be any odd prime different from τ. If p is a quadratic residue modulo τ, then $pt \in \mathfrak{K}'_{m,n}$, for some $t \in \mathbb{Z}$. If $p > \sqrt{\frac{\tau}{3}}$, then we may assume that $0 < |t| < p$.*

Proof. By Lemma 4.1, there is some $r \in \mathbb{Z}$ such that $r^2 \equiv m^2 - 4n \pmod p$. Choose $s \in \mathbb{Z}$ such that $2s + m \equiv r \pmod p$. We have $4s^2 + 4ms + 4n \equiv 0 \pmod p$, and hence $s^2 + ms + n \equiv 0 \pmod p$. Hence, for some $t' \in \mathbb{Z}$, there is representation $t'p = f(s, 1)$.

We return now to the choice of s, and try to find a different choice (but still equivalent modulo p), which will make $|t'|$ small. Consider the quadratic real, integer-valued, polynomial $g(x) = (s + xp)^2 + m(s + xp) + n$. For all $x \in \mathbb{Z}$, $g(x)$ will not only be integer-valued, but a multiple of p. $g(x)$ has vertex at $k' = -\frac{2s-m}{2p}$. We calculate $g(k') = \frac{4n-m^2}{4}$, and $g(k' + \frac{1}{2}) = g(k' - \frac{1}{2}) = \frac{4n-m^2}{4} + \frac{p^2}{4}$. Choose an integer $k \in [k' - \frac{1}{2}, k' + \frac{1}{2}]$. We have $g(k) \in [\frac{4n-m^2}{4}, \frac{4n-m^2}{4} + \frac{p^2}{4}]$. Hence, $|g(k)| \leq |\frac{4n-m^2}{4}| + |\frac{p^2}{4}| = \frac{\tau}{4} + \frac{p^2}{4} < \frac{3p^2}{4} + \frac{p^2}{4} = p^2$. Hence, for some t with $|t| < p$, we have $tp = g(k) = f(k, 1)$. We have $t \neq 0$ since $0 \notin \mathfrak{K}'_{m,n}$. □

This next lemma is a generalization of a result found in [3]. It shows that if prime p and pt are both representable, then t is also representable.

Lemma 4.5. *Let $m, n \in \mathbb{Z}$ with $\tau = |m^2 - 4n|$ prime. Let $t, p \in \mathbb{N}$ with p prime. If $tp, p \in \mathfrak{K}_{m,n}$, then $t \in \mathfrak{K}_{m,n}$.*

Proof. By hypothesis, there are integers a, b, c, d with $tp = a^2 + mab + nb^2$ and $p = c^2 + mcd + nd^2$. Since p is prime, in fact $\gcd(c, d) = 1$. We calculate $b^2p - d^2tp = b^2(c^2 + mcd + nd^2) - d^2(a^2 + mab + nb^2) = (bc - ad)(mbd + bc + ad)$. Hence either $p|(bc - ad)$ or $p|(mbd + bc + ad)$, which splits the proof into two cases.

Suppose first that $p|(bc - ad)$. There is some $r \in \mathbb{Z}$ with $rp = bc - ad$. Set $y = a + rnd$ and $x = b - rc$. We substitute for a, b to get $rp = r(c^2 + mcd + nd^2) - rmcd - yd + xc$, so $0 = -rmcd - yd + xc$ and hence $c(x - rmd) = dy$. Since $\gcd(c, d) = 1$, there is some $w \in \mathbb{Z}$ with $y = cw$. Substituting, we get $x = d(w+rm)$. Hence $a = cw - rnd$ and $b = d(w + rm) + rc$. We claim that $t = w^2 + mwr + nr^2$, since $(w^2 + mwr + nr^2)(c^2 + mcd + nd^2) = (cw - rnd)^2 + m(cw - rnd)(d(w + rm) + rc) + n(d(w + rm) + rc)^2 = a^2 + mab + nb^2 = tp$.

Suppose now that $p|(mbd+bc+ad)$. There is some $r \in \mathbb{Z}$ with $rp = mbd+bc+ad$. Set $y = a - rnd$ and $x = b - rc$. We substitute for a, b to get $rp = r(c^2 + mcd + nd^2) + mxd + xc + yd$, so $0 = mxd + xc + yd$ and hence $d(mx + y) = c(-x)$. Since $\gcd(c, d) = 1$, there is some $w \in \mathbb{Z}$ with $-x = dw$. Substituting, we get $y = w(dm + c)$. Hence $a = w(dm + c) + rnd$ and $b = -dw + rc$. We claim that $t = w^2 + mwr + nr^2$, since $(w^2 + mwr + nr^2)(c^2 + mcd + nd^2) = (w(dm + c) + rnd)^2 + m(w(dm + c) + rnd)(-dw + rc) + n(-dw + rc)^2 = a^2 + mab + nb^2 = tp$.□

We now prove that all primes that are quadratic residues are representable, subject to Condition P.

Theorem 4.6. *Let $m, n \in \mathbb{Z}$ with $\tau = |m^2 - 4n|$ prime. Suppose that Condition P holds. Then $p \in \mathfrak{K}_{m,n}$ for every prime p that is a quadratic residue modulo τ.*

Proof. By way of contradiction, let p be the smallest prime with $\left(\frac{p}{\tau}\right) = 1$ and $p \notin \mathfrak{K}_{m,n}$. If $p \leq \sqrt{\frac{\tau}{3}}$, then $p \in \mathfrak{P}_\tau$, which contradicts Condition P.

We now choose $t \in \mathbb{Z}$ to have minimal absolute value to satisfy both $0 < |t| < p$ and $pt \in \mathfrak{K}'_{m,n}$. Note that such a t exists by Lemma 4.4.

If $t = 1$ we contradict $p \notin \mathfrak{K}_{m,n}$. If τ is of Type I, $t = -1$ is impossible by Lemma 3.4. If τ is of Type II and $t = -1$, then, by Condition P, $-1 \in \mathfrak{K}_{m,n}$. Applying Lemma 2.2, $p = (-1)(tp) \in \mathfrak{K}_{m,n}$, a contradiction. Hence we may assume that $|t| > 1$ and write $|t| = p_1p_2 \cdots p_k$, a product of (not necessarily distinct) primes, each less than p.

Suppose that some $p_i \in \mathfrak{K}_{m,n}$; we will show that this is impossible. By Lemma 4.5, $p\frac{t}{p_i} \in \mathfrak{K}_{m,n}$. Hence $p\frac{t}{p_i} = a^2 + mab + nb^2$ for some $a, b \in \mathbb{Z}$. We have $\gcd(a, b)^2 | p\frac{t}{p_i}$. If $\gcd(a, b) = p$, then $p^2|pt$, a contradiction. Hence $\gcd(a, b)^2 | \frac{t}{p_i}$. We now have $p\frac{t}{p_i \gcd(a,b)^2} = (\frac{a}{\gcd(a,b)})^2 + m(\frac{a}{\gcd(a,b)})(\frac{b}{\gcd(a,b)}) + n(\frac{n}{\gcd(a,b)})^2 \in \mathfrak{K}'_{m,n}$. This contradicts our choice of t. Hence each $p_i \notin \mathfrak{K}_{m,n}$ and in particular $p_i \neq \tau$.

Hence, each p_i is a quadratic nonresidue modulo τ, otherwise by our choice of p we must have $p_i \in \mathfrak{K}_{m,n}$. If any p_i were odd, this would contradict Lemma 4.2. Hence $t = 2^c$ for some $c \in \mathbb{N}$, where 2 is a quadratic nonresidue modulo τ. If $c = 1$, then $tp = 2p$ is the product of a quadratic nonresidue and a quadratic residue. Hence tp

is a quadratic nonresidue, and by Theorem 3.1, $tp \notin \mathfrak{K}_{m,n}$, a contradiction. Hence $c \geq 2$, but by Lemma 4.3, $tp = 4(2^{c-2}p) \notin \mathfrak{K}'_{m,n}$, a contradiction. □

We can now reproduce the known results. For the known $\tau = 3$, of Type I, $\mathfrak{P}_3 = \emptyset$, and Condition P holds vacuously. For the known $\tau(-1,-1) = 5$, $\mathfrak{P}_5 = \{-1, 5\}$. -1 is representable by Lemma 3.2, so to check Condition P we need only find $5 = f(3,1)$. For another example, take $\tau(3,-2) = 17$. We have $\mathfrak{P}_{17} = \{-1, 2, 17\}$. -1 is again representable by Lemma 3.2, so Condition P is verified once we find $2 = f(1,1)$ and $17 = f(5,8)$.

We turn now to the question of characterizing irreducibles in the monoid $\mathfrak{K}_{m,n}$. Due to Lemmas 3.3 and 3.4, we concern ourselves only with irreducibles in $\mathfrak{K}_{m,n} \cap \mathbb{N}$, itself a monoid.

Lemma 4.7. *Let $m, n \in \mathbb{Z}$ with $\tau = |4n - m^2|$ prime. Suppose that Condition P holds. Then the irreducibles in monoid $\mathfrak{K}_{m,n} \cap \mathbb{N}$ are exactly those integers of the form:*

(1) p, where p is prime and a quadratic residue modulo τ; and
(2) q^2, where q is prime and a quadratic nonresidue modulo τ.

Proof. We have $p \in \mathfrak{K}_{m,n}$ by Theorem 4.6. We have $q^2 = f(q,0) \in \mathfrak{K}_{m,n}$; it is irreducible by Theorem 3.1. Now let $t \in \mathfrak{K}_{m,n}$ be some other irreducible. Write $t = p_1 p_2 \cdots p_k$, for not necessarily distinct primes p_i. We must have $k \geq 2$ by Theorem 3.1 again. If any $p_i \in \mathfrak{K}_{m,n}$, then by Lemma 4.5, $\frac{t}{p_i} \in \mathfrak{K}_{m,n}$, which contradicts irreducibility. In particular, by Condition P, no p_i can be τ. If any p_i is odd, then by Lemma 4.2, $t \notin \mathfrak{K}'_{m,n}$. But then, writing $t = a^2 + mab + nb^2$, there is some prime r dividing $\gcd(a,b)$. We have $r^2 = f(r,0)$ and $\frac{t}{r^2} = (\frac{a}{r})^2 + m(\frac{a}{r})(\frac{b}{r}) + n(\frac{b}{r})^2$. But $\frac{t}{r^2} > 1$ since t is not among the two types of irreducibles already described. Hence t is reducible, which is a contradiction. The remaining possibility is that t is a power of 2, where 2 is a quadratic nonresidue. An even power of 2 may be written as a product of irreducibles 2^2, while an odd power of 2 is not in $\mathfrak{K}_{m,n}$ by Theorem 3.1. Hence no such t can exist. □

With the irreducibles we may easily determine the full monoid $\mathfrak{K}_{m,n}$. The statement of Theorem 4.8 is similar to a well-known theorem on representing integers as the sum of two squares, i.e. the quadratic form $4 = \tau(0,1)$. We recall also Lemmas 3.3 and 3.4, which combine with Theorem 4.8 to resolve the membership question for negative integers.

Theorem 4.8. *Let $m, n \in \mathbb{Z}$ with $\tau = |4n - m^2|$ prime. Suppose that Condition P holds. Let $t \in \mathbb{N}$. Then $t \in \mathfrak{K}_{m,n}$ if and only if the prime decomposition of t contains no prime, that is a quadratic nonresidue modulo τ, raised to an odd power.*

Proof. Immediate from Lemma 4.7. □

References

[1] K. Bahmanpour, Prime numbers p with expression $p = a^2 \pm ab \pm b^2$, J. Number Theory 166 (2016) 208–218.
URL `https://doi.org/10.1016/j.jnt.2016.02.024`

[2] G. H. Hardy, E. M. Wright, An introduction to the theory of numbers, sixth Edition, Oxford University Press, Oxford, 2008, revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.

[3] U. P. Nair, Elementary results on the binary quadratic form $a^2 + ab + b^2$ (2004). arXiv:arXiv:math/0408107.