ON THE MONOID OF MONIC BINARY QUADRATIC FORMS

JEROME T. DIMABAYAO, VADIM PONOMARENKO,
AND ORLAND JAMES Q. TIGAS

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

1. 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 $f_{m,n}(x, y) := x^2 + mxy + ny^2$, 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 $f_{m,n}(x, y)$ represents.

Modern knowledge about quadratic forms comes from the genus theory of Gauss and also involves the geometry of numbers and factorization over rings of integers of number fields. But it is still interesting to ask how far elementary methods can go for the study of such forms. For instance, although it is well-known that the product of two sums of squares is a sum of squares, the fact that it extends to products of arbitrary monic binary quadratic forms seems to be less-known (cf. [1]).

This problem was revisited by Nair [4] for the form $\tau(1, 1) = 3$. More recently, Bahmanpour [1] determined the primes represented by forms $\tau(1, 1) = 3$ and $\tau(1, -1) = 5$. We extend these results to all forms with prime τ, provided Condition P holds (as defined below). All the above-mentioned results were obtained by elementary arguments using the fact that the set of integers represented by τ forms a monoid under multiplication of integers (see Lemma 1 below).

2010 *Mathematics Subject Classification.* 11N32, 11E25, 11A41.

Key words and phrases. Binary quadratic form; Law of quadratic reciprocity; prime number.

We have verified condition P, computationally, for the following values:

$$\tau = 3, 5, 7, 11, 13, 17, 19, 23, 29, 37, 41, 43, 53, 61, 67, 101, 163, 173, 197.$$

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 the case where τ is 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 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. For $m, n \in \mathbb{Z}$, let $\mathfrak{K}_{m,n} := \{x^2 + mxy + ny^2 : x, y \in \mathbb{Z}\}$ denote the set of representable integers. This set is a monoid under multiplication.

Lemma 1 (from [1])**.** *Let $m, n \in \mathbb{Z}$. 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 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 and n. For example, $5 = \tau(1, -1) = \tau(3, 1)$.

The following lemma shows that we may assume that the coefficient of the cross term is one for the quadratic forms that we want to study.

Lemma 2. *Let $m, n \in \mathbb{Z}$ such that $\tau = |m^2 - 4n|$ is odd. We have $\mathfrak{K}_{m,n} = \mathfrak{K}_{1, \frac{1-(m^2-4n)}{4}}$.*

Proof. If τ is odd, then m is also odd. Now suppose $t = a^2 + mab + nb^2 \in \mathfrak{K}_{m,n}$. If we put $c = a - \left(\frac{1-m}{2}\right) b \in \mathbb{Z}$, then we see that $t = c^2 + cb + \frac{1-(m^2-4n)}{4} b^2 \in \mathfrak{K}_{1, \frac{1-(m^2-4n)}{4}}$. Conversely, if $s = x^2 + xy + \frac{1-(m^2-4n)}{4} y^2 \in \mathfrak{K}_{1, \frac{1-(m^2-4n)}{4}}$, then $s = z^2 + mzy + ny^2 \in \mathfrak{K}_{m,n}$, where $z = x + \left(\frac{1-m}{2}\right) y$.

□

In view of the above result, we put $\mathfrak{K}_n := \mathfrak{K}_{1,n} = \{x^2 + xy + ny^2 : x, y \in \mathbb{Z}\}$. We define $\mathfrak{K}'_n := \{x^2 + xy + ny^2 : x, y \in \mathbb{Z}, \gcd(x, y) = 1\}$, a subset of $\mathfrak{K}_n$. Note that all nonzero squarefree elements of $\mathfrak{K}_n$ are in $\mathfrak{K}'_n$ (in particular, all primes in $\mathfrak{K}_n$). Theorem 3 will prove that $\mathfrak{K}_n$ depends only on τ and Condition P, to be defined below.

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

$$\mathfrak{P}_\tau := \left\{ p \text{ prime} : p \leq \sqrt{\frac{\tau}{3}}, \left(\frac{p}{\tau}\right) = 1 \right\}.$$

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

$$\mathfrak{P}_\tau \subseteq \mathfrak{K}_n. \qquad \text{(Condition P)}$$

We determine all representable primes (in Theorems 1 and 2). We then find all representable integers (in Theorem 3). A prime turns out to be representable in $\mathfrak{K}_n$ if and only if it is equal to τ or 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.

2. 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 1. *Let $n, t \in \mathbb{Z}$ such that $\tau = |4n-1|$ is prime and $\tau \nmid t$. Suppose that t is a quadratic nonresidue modulo τ. Then $t \notin \mathfrak{K}_n$.*

Proof. By way of contradiction, let us assume the existence of $a, b \in \mathbb{Z}$ with $t = a^2 + ab + nb^2$. Multiplying both sides by 4 and working modulo τ, we have $4t \equiv 4a^2 + 4ab + 4nb^2 \equiv (2a+b)^2 + b^2(4n-1) \equiv (2a+b)^2$. 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 $f_{1,n}(-1,2) = (-1)^2 + (-1)2 + 4n = -1 + 4n = \tau$. If τ is of Type II, there is no such immediate formula. For example, $37 = \tau(1,-9) \in \mathfrak{K}_{-9}$ as $37 = f_{1,-9}(31,12)$. For the slightly larger prime $97 = \tau(1,-24) \in \mathfrak{K}_{-24}$ as $97 = f_{1,-24}(-60797, 11208)$. But the same expression $f_{1,n}(-1,2)$ as above shows that $-\tau$ is represented when τ is of Type II. We thus obtain representability for τ in this case if we can verify representability for -1. We attain this using the following known result, whose proof will be included for completeness.

Lemma 3. *Let p be a prime with $p \equiv 1 \pmod 4$. Then there exist $x, y \in \mathbb{N}$ such that $x^2 - py^2 = -1$.*

Proof. By a theorem of Lagrange (cf. e.g. [3, Thm. 1, p. 53]), there exist infinitely many pairs of positive integers $(X, Y) \neq (1, 0)$ that satisfies the Pell equation

$$X^2 - pY^2 = 1. \tag{2.1}$$

Consider such a pair (X_0, Y_0) with minimal X_0. Note that X_0 and Y_0 are relatively prime. Since $p \equiv 1 \pmod 4$, X_0 must be odd and Y_0 is even. Write $Y_0 = 2W$. Then we may write equation (2.1) as

$$\frac{X_0 + 1}{2} \cdot \frac{X_0 - 1}{2} = pW^2.$$

Since $\frac{X_0+1}{2} - \frac{X_0-1}{2} = 1$, the integers $\frac{X_0+1}{2}$ and $\frac{X_0-1}{2}$ must be relatively prime. Hence, there exist relatively prime positive integers a and b such that

$$\begin{cases} \frac{X_0+1}{2} = a^2 \\ \frac{X_0-1}{2} = pb^2 \end{cases} \qquad \text{or} \qquad \begin{cases} \frac{X_0+1}{2} = pa^2 \\ \frac{X_0-1}{2} = b^2. \end{cases}$$

In the first case we have $X_0 = 2a^2 - 1 = 2pb^2 + 1$, which gives $a^2 - pb^2 = 1$. But we also have

$$1 \leq a \leq a^2 \leq 2a^2 - 1 = X_0.$$

This contradicts the minimality of X_0 and the assumption that $X_0 \neq 1$. Hence we must have $X_0 = 2pa^2 - 1 = 2b^2 + 1$, which gives $b^2 - pa^2 = -1$. □

Lemma 4. *Let $n \in \mathbb{Z}$ such that $\tau = 1 - 4n$ is a prime of type II. Then $-1 \in \mathfrak{K}_n$.*

Proof. Let $x, y \in \mathbb{N}$ such that $x^2 - \tau y^2 = -1$. Then we find $f_{1,n}(-x - y, 2y) = (x + y)^2 - (x + y)(2y) + 4ny^2 = x^2 - (1 - 4n)y^2 = -1$. □

Using Lemma 4, we see that monoids of type II are nicely symmetric around 0.

Lemma 5. *Let $m, n \in \mathbb{Z}$ such that $\tau = 1 - 4n$ is a prime of type II. Then for every $t \in \mathbb{Z}$, $t \in \mathfrak{K}_n$ if and only if $-t \in \mathfrak{K}_n$. In particular, $\tau \in \mathfrak{K}_n$.*

Proof. Apply Lemma 1 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 6. *Let $n \in \mathbb{Z}$ such that $\tau = 4n-1$ is a prime of type I. Then $\mathfrak{K}_n \subseteq \mathbb{N}_0$.*

Proof. Let $a, b \in \mathbb{Z}$. Since $4n > 1$, we must have $n > 0$. Set $s = \frac{1}{\sqrt{n}}$, and $c = b\sqrt{n}$. We have $a^2+ab+nb^2 = a^2+sac+c^2 = \frac{2+s}{4}(a+c)^2+\frac{2-s}{4}(a-c)^2$. Since $4n > 1$, $|s| < 2$ and hence both $\frac{2+s}{4}$ and $\frac{2-s}{4}$ are positive. Thus $a^2+ab+nb^2 \geq 0$, with equality only for $a = b = 0$. □

3. Representing Quadratic Residues

We turn now to the question of representing quadratic residues. This is less straightforward than Theorem 1, as not all quadratic residues are representable. In several steps we prove Theorem 2, which resolves representation of primes that are quadratic residues.

The next lemma, relying on the law of quadratic reciprocity, is the starting point toward Theorem 2. It will be needed for all primes except 2 and τ.

Lemma 7. *Let $n \in \mathbb{Z}$ such that $\tau = |1 - 4n|$ is a prime. Let p be any odd prime different from τ. Then p is a quadratic residue modulo τ if and only if $1 - 4n$ is a quadratic residue modulo p.*

Proof. Suppose first that $1 - 4n > 0$. By quadratic reciprocity,

$$1 = \left(\frac{1-4n}{p}\right)\left(\frac{p}{1-4n}\right),$$

since $1 - 4n \equiv 1 \pmod 4$. On the other hand, if $1 - 4n < 0$, then

$$(-1)^{(p-1)/2} = \left(\frac{\tau}{p}\right)\left(\frac{p}{\tau}\right),$$

since $\tau \equiv -(1 - 4n) \equiv -1 \pmod 4$. But also

$$\left(\frac{\tau}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{1-4n}{p}\right) = (-1)^{(p-1)/2}\left(\frac{1-4n}{p}\right).$$

This implies

$$1 = \left(\frac{1-4n}{p}\right)\left(\frac{p}{\tau}\right).$$

□

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

Lemma 8. *Let $n \in \mathbb{Z}$ such that $\tau = |1 - 4n|$ is a 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 $pt \notin \mathfrak{K}'_n$.*

Proof. We assume by way of contradiction the existence of $a, b \in \mathbb{Z}$ with $pt = a^2 + ab + nb^2$ and $\gcd(a, b) = 1$. If $p|b$, then $p|(pt - ab - nb^2)$, 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 $0 \equiv a^2 + ab + nb^2 \equiv$

$b^2((ac)^2 + (ac) + n)$. Hence $0 \equiv 4((ac)^2 + (ac) + n) \equiv (2ac + 1)^2 + 4n - 1$, and thus $(2ac + 1)^2 \equiv 1 - 4n \pmod{p}$. Thus $1 - 4n$ is a quadratic residue, modulo p. By Lemma 7, p is a quadratic residue modulo τ; this contradicts the 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 8 to this p and to $t = 0$, implies that $0 \notin \mathfrak{K}'_n$.

We now present an analogue of Lemma 8 for $p = 2$.

Lemma 9. *Let $n, t \in \mathbb{Z}$ such that $\tau = |1 - 4n|$ is a prime. If 2 is a quadratic nonresidue modulo τ, then $4t \notin \mathfrak{K}'_n$.*

Proof. Since $\left(\frac{2}{\tau}\right) = -1$, by the second supplement to the law of quadratic reciprocity, we must have $|1 - 4n| = \tau \equiv \pm 3 \pmod{8}$. A simple case analysis shows that n is odd. Assume by way of contradiction the existence of $a, b \in \mathbb{Z}$ with $4t = a^2 + ab + nb^2$ and $\gcd(a, b) = 1$. In particular, a, b cannot both be even. If a, b are both odd, then $a^2+ab+nb^2$ is also odd, a contradiction. If b is odd and $a = 2k$ is even, we have $0 \equiv (2k)^2+(2k)b+nb^2 \equiv b(2k+nb) \pmod{4}$. But now $4|(2k+nb)$, so nb is even and hence b is even, a contradiction. Lastly, if a is odd and $b = 2j$ is even, we have $0 \equiv a^2 + a(2j) + n(2j)^2 \equiv a(a + 2j) \pmod{4}$. But now $4|(a + 2j)$, 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 10. *Let $n \in \mathbb{Z}$ such that $\tau = |1 - 4n|$ is a prime. Let p be any odd prime different from τ. If p is a quadratic residue modulo τ, then $pt \in \mathfrak{K}'_n$, for some $t \in \mathbb{Z}$. If $p > \sqrt{\frac{\tau}{3}}$, then we may assume that $0 < |t| < p$.*

Proof. By Lemma 7, there is some $r \in \mathbb{Z}$ such that $r^2 \equiv 1 - 4n \pmod{p}$. Choose $s \in \mathbb{Z}$ such that $2s + 1 \equiv r \pmod{p}$. We have $4s^2 + 4s + 4n \equiv 0 \pmod{p}$, and hence $s^2 + s + n \equiv 0 \pmod{p}$. Hence, for some $t' \in \mathbb{Z}$, there is a representation $t'p = f_{1,n}(s, 1)$.

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 polynomial $g(x) = (s + xp)^2 + (s + xp) + n$. For all $x \in \mathbb{Z}$, $g(x)$ will not only be integer-valued, but a multiple of p. The graph of $g(x)$ has vertex at $k' = -\frac{2s+1}{2p}$. We calculate $g(k') = \frac{4n-1}{4}$, and $g(k' + \frac{1}{2}) = g(k' - \frac{1}{2}) = \frac{4n-1}{4} + \frac{p^2}{4}$. Choose an integer $k \in [k' - \frac{1}{2}, k' + \frac{1}{2}]$. We have $g(k) \in [\frac{4n-1}{4}, \frac{4n-1}{4} + \frac{p^2}{4}]$. Hence, $|g(k)| \leq |\frac{4n-1}{4}| + |\frac{p^2}{4}| = \frac{\tau}{4} + \frac{p^2}{4} < \frac{3p^2}{4} + \frac{p^2}{4} = p^2$. Hence, for some t with $|t| < p$, we have $tp = g(k) = f_{1,n}(s + kp, 1)$. We have $t \neq 0$ since $0 \notin \mathfrak{K}'_n$. □

This next lemma is a generalization of a result found in [4]. It shows that if a prime p and pt, for some $t \in \mathbb{Z}$, are both representable, then t is also representable.

Lemma 11. *Let $n \in \mathbb{Z}$, $t \in \mathbb{N}$ and p be a prime. If $tp, p \in \mathfrak{K}_n$, then $t \in \mathfrak{K}_n$.*

Proof. By hypothesis, there are integers a, b, c, d with $tp = a^2 + ab + nb^2$ and $p = c^2 + cd + nd^2$. In fact we have $\gcd(c, d) = 1$, since p is prime. We calculate $b^2p - d^2tp = b^2(c^2 + cd + nd^2) - d^2(a^2 + ab + nb^2) = (bc - ad)(bd + bc + ad)$. Hence either $p|(bc - ad)$ or $p|(bd + bc + ad)$, 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 $rp = r(c^2 + cd + nd^2) - rcd - yd + xc$, so $0 = -rcd - yd + xc$ and hence $c(x - rd) = dy$. Since $\gcd(c, d) = 1$, there is some $w \in \mathbb{Z}$ with $y = cw$. Substituting, we get $x = d(w + r)$. Hence $a = cw - rnd$ and $b = d(w + r) + rc$. Since $(w^2 + wr + nr^2)(c^2 + cd + nd^2) = (cw - rnd)^2 + (cw - rnd)(d(w + r) + rc) + n(d(w + r) + rc)^2 = a^2 + ab + nb^2 = tp$, we find that $t = w^2 + wr + nr^2 \in \mathfrak{K}_n$.

Suppose now that $p|(bd+bc+ad)$. There is some $r \in \mathbb{Z}$ with $rp = bd+bc+ad$. Set $y = a - rnd$ and $x = b - rc$. We substitute for a, b to get $rp = r(c^2 + cd + nd^2) + xd + xc + yd$, so $0 = xd + xc + yd$ and hence $d(x + y) = c(-x)$. Since $\gcd(c, d) = 1$, there is some $w \in \mathbb{Z}$ with $-x = dw$. Substituting, we get $y = w(d + c)$. Hence $a = w(d + c) + rnd$ and $b = -dw + rc$. Since $(w^2 + wr + nr^2)(c^2 + cd + nd^2) = (w(d + c) + rnd)^2 + (w(d + c) + rnd)(-dw + rc) + n(-dw + rc)^2 = a^2 + ab + nb^2 = tp$, we find that $t = w^2 + wr + nr^2 \in \mathfrak{K}_n$. □

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

Theorem 2. *Let $n \in \mathbb{Z}$ such that $\tau = |1 - 4n|$ is a prime. Suppose that Condition P holds. Then $p \in \mathfrak{K}_n$ 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 $p \notin \mathfrak{K}_n$. 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 $pt \in \mathfrak{K}'_n$. Note that such a t exists by Lemma 10.

If $t = 1$ we contradict $p \notin \mathfrak{K}_n$. If τ is of Type I, $t = -1$ is impossible by Lemma 6. Suppose τ is of Type II and $t = -1$. From Lemma 4 we have $-1 \in \mathfrak{K}_n$. Thus Lemma 1 gives $p = (-1)(tp) \in \mathfrak{K}_n$, 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 $p_i \in \mathfrak{K}_n$; we will show that this is impossible. By Lemma 11, $p\frac{t}{p_i} \in \mathfrak{K}_n$. Hence $p\frac{t}{p_i} = a^2 + ab + nb^2$ 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 $\frac{pt}{p_i \gcd(a,b)^2} = \left(\frac{a}{\gcd(a,b)}\right)^2 + \left(\frac{a}{\gcd(a,b)}\right)\left(\frac{b}{\gcd(a,b)}\right) + n\left(\frac{b}{\gcd(a,b)}\right)^2 \in \mathfrak{K}'_n$. This contradicts our choice of t. Hence each $p_i \notin \mathfrak{K}_n$ and in particular $p_i \neq \tau$.

Consequently each p_i is a quadratic nonresidue modulo τ, otherwise by our choice of p we must have $p_i \in \mathfrak{K}_n$. If any p_i were odd, we would obtain a contradiction to Lemma 8. 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 1, $tp \notin \mathfrak{K}_n$, a contradiction. Hence $c \geq 2$, but by Lemma 9, $tp = 4(2^{c-2}p) \notin \mathfrak{K}'_n$, a contradiction. □

We can now reproduce the known results. For the known $\tau(1,1) = 3$ of Type I and $\tau(-1,-1) = \tau(1,-1) = 5$ of type II, we have $\mathfrak{P}_3 = \emptyset$ and $\mathfrak{P}_5 = \emptyset$, respectively. Thus, condition P holds vacuously for these two examples. For another example, take $17 = \tau(3,-2) = \tau(1,-4)$. We have $\mathfrak{P}_{17} = \{2\}$. Then condition P is verified since $2 = f_{1,-4}(2,1)$. We also have $2 = f_{3,-2}(1,1)$ by inspection (or using the proof of Lemma 2).

4. Complete determination of representable integers

We turn now to the question of characterizing irreducibles in the monoid $\mathfrak{K}_n$. Due to Lemmas 5 and 6, we concern ourselves only with irreducibles in $\mathfrak{K}_n \cap \mathbb{N}$, itself a monoid.

Lemma 12. *Let $n \in \mathbb{Z}$ such that $\tau = |1 - 4n|$ is a prime. Suppose that Condition P holds. Then the irreducibles in the monoid $\mathfrak{K}_n \cap \mathbb{N}$ are exactly those integers of the form:*

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

Proof. We have $\tau \in \mathfrak{K}_n$ from Section 2 and $p \in \mathfrak{K}_n$ by Theorem 2. We have $q^2 = f_{1,n}(q,0) \in \mathfrak{K}_n$; it is irreducible by Theorem 1. Now let $t \in \mathfrak{K}_n$ 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 1 again. If any $p_i \in \mathfrak{K}_n$, then by Lemma 11, $\frac{t}{p_i} \in \mathfrak{K}_n$, which contradicts irreducibility. In particular, by Condition P, no p_i can be τ. If any p_i is odd, then by Lemma 8, $t \notin \mathfrak{K}'_n$. But then, writing $t = a^2 + ab + nb^2$, there is some prime r dividing $\gcd(a,b)$. We have $r^2 = f_{1,n}(r,0)$ and $\frac{t}{r^2} = (\frac{a}{r})^2 + (\frac{a}{r})(\frac{b}{r}) + n(\frac{b}{r})^2$. 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 modulo τ. An even power of 2 may be written as a

product of irreducibles 2^2, while an odd power of 2 is not in $\mathfrak{K}_n$ by Theorem 1. Hence no such t can exist. □

With the irreducibles we may easily determine the full monoid $\mathfrak{K}_n$. The statement of Theorem 3 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 5 and 6, which combine with Theorem 3 to resolve the membership question for negative integers.

Theorem 3. *Let $n \in \mathbb{Z}$ such that $\tau = |1 - 4n|$ is a prime. Suppose that Condition P holds. Let $t \in \mathbb{N}$. Then $t \in \mathfrak{K}_n$ 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 12. □

References

[1] K. Bahmanpour, "Prime numbers p with expression $p = a^2 \pm ab \pm b^2$." *J. Number Theory*, vol. 166, pp. 208–218, 2016, doi: 10.1016/j.jnt.2016.02.024.

[2] G. Hardy and E. Wright, *An introduction to the theory of numbers. Edited and revised by D. R. Heath-Brown and J. H. Silverman. With a foreword by Andrew Wiles. 6th ed.*, 6th ed. Oxford: Oxford University Press, 2008.

[3] L. Mordell, "Diophantine equations." Pure and Applied Mathematics, 30. London-New York: Academic Press. x, 312 p. (1969).

[4] U. P. Nair, "Elementary results on the binary quadratic form $a^2 + ab + b^2$," 2004.

Institute of Mathematics, College of Science, University of the Philippines Diliman, C.P. Garcia St., U.P.Campus, Diliman, 1101 Quezon City, Philippines
E-mail address: jdimabayao@math.upd.edu.ph

Department of Mathematics and Statistics, San Diego State University, 5500 Campanile Drive, San Diego California, USA
E-mail address: vponomarenko@mail.sdsu.edu

Institute of Mathematics, College of Science, University of the Philippines Diliman, C.P. Garcia St., U.P.Campus, Diliman, 1101 Quezon City, Philippines
E-mail address: oqtigas@upd.edu.ph