EXPLICIT SOLUTIONS FOR $u^2 - pv^2 = \pm 2$ AND A CONJECTURE OF MORDELL

DEBOPAM CHAKRABORTY AND ANUPAM SAIKIA

Abstract. We obtain an explicit solution of the Pell’s equation $u^2 - pv^2 = \pm 2$ in terms of the convergents of the continued fraction of the prime $p$. Then we show that Mordell’s conjecture concerning the fundamental unit of $\mathbb{Q}(\sqrt{p})$ holds for the three conjecturally infinite families of primes $p$. As a consequence of our approach, we provide an alternative proof for the following facts concerning the period of the continued fraction of $\sqrt{p}$: (i) the length of the period of $\sqrt{p}$ is divisible by 4 when $p$ is a prime congruent to 7 modulo 8, (ii) the length is of the form $4k + 2$ when $p$ is a prime congruent to 3 modulo 8, (iii) the central term in the palindromic part of the period of $\sqrt{p}$ is the largest odd integer not exceeding $\sqrt{p}$ for $p \equiv 3 \mod 4$.

1. Introduction

The Pell’s equation $u^2 - dy^2 = N$ for an integer $d > 1$ has a rich history. The integral solutions for $N = \pm 1$ or $N = \pm 4$ provide us the units in the ring of integers of $\mathbb{Q}(\sqrt{d})$. It is well-known that the integral solutions for $N = \pm 1$ can be explicitly described in terms of the continued fraction expansion of $\sqrt{d}$. In this article, we first consider the equation $u^2 - pv^2 = \pm 2$ for primes $p$ congruent to 3 modulo 4. It is known that there exist solutions for $u^2 - pv^2 = 2$ when $p \equiv 7 \mod 8$ and a solutions for $u^2 - pv^2 = -2$ when $p \equiv 3 \mod 8$ (e.g., see [8]). We provide the solutions for these equations explicitly in terms of the convergents of the continued fraction of $\sqrt{p}$ by theorem 5.2.

We also discuss certain applications of our results in propositions 7.1, 7.2 and corollaries 7.3, 7.4, 7.5. In particular, we show that Mordell’s Conjecture concerning the fundamental unit of $\mathbb{Q}(\sqrt{p})$ holds when $\sqrt{p}$ has period of length 2, 4 or 6. Mordell’s conjecture states that if $\xi_p = x + y\sqrt{p}$ is the fundamental unit of $\mathbb{Q}(\sqrt{p})$ for a prime $p$ congruent to 3 modulo 4, then $p$ does not divide $y$ ([10]). This conjecture is preceded by a famous conjecture of Ankeny, Artin and Chowla in [1], which predicted non-divisibility in the case when $p$ is a prime congruent to 3 modulo 4.
SOLUTIONS FOR $u^2 - pv^2 = \pm 2$ AND MORDELL’S CONJECTURE

2. THE CONVERGENTS OF $\sqrt{p}$

We first establish certain recurrence relation that hold for the convergents of the continued fraction of $\sqrt{p}$ for any prime $p$. Let

$$\sqrt{p} = \langle n, a_1, a_2, \ldots, a_r, 2n \rangle.$$

We denote it as $\sqrt{p} = \langle n, a_1, a_2, \ldots, a_r, 2n \rangle$. Here, the first $r$ terms $a_1, a_2, \ldots, a_r$ of the period $(a_1, a_2, \ldots, a_r, 2n)$ form a palindrome. We establish a deeper relation between the continued fraction of $\sqrt{p}$ and the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{p})$ that yield our results (see proposition 5.1). Our approach provides an alternative proof that the length $r + 1$ of the period is of the form $4k$ when $p \equiv 7$ modulo 8 and of the form $4k + 2$ when $p \equiv 3$ mod 8 (see proposition 4.1). We can further show that the central term $a_{r+1}^{(2)}$ is the largest odd integer not exceeding $\sqrt{p}$ (see corollary 6.2).
The $i$-th convergent of the continued fraction of $\sqrt{p}$ is given by

\begin{equation}
\frac{k_i}{h_i} = n + \frac{1}{a_1 + \frac{1}{a_2 + \cdots + \frac{1}{a_i}}}.
\end{equation}

We can write the first few convergents as

\begin{equation}
\begin{align*}
h_0 &= 1, \quad k_0 = n; \quad h_1 = a_1, \quad k_1 = na_1 + 1; \\
h_2 &= 1 + a_1a_2, \quad k_2 = na_1a_2 + n + a_2.
\end{align*}
\end{equation}

By convention, we take $h_{-1} = 0, \quad k_{-1} = 1$.

The following recurrence relations satisfied by $k_i$ and $h_i$ are easy to verify.

\begin{equation}
k_{i+1} = a_{i+1}k_i + k_{i-1}, \quad k_{i+1} = a_{i+1}k_i + k_{i-1} \quad \text{for} \quad i \geq 2.
\end{equation}

It can be readily verified that

\begin{equation}
k_r = nh_r + h_{r-1}.
\end{equation}

The following relations involving the convergents are well-known and can be easily proved (see [3]):

\begin{equation}
k_i h_{i-1} - k_{i-1} h_i = (-1)^{i-1} \quad \text{for} \quad i \geq 0
\end{equation}

\begin{equation}
(nh_r + h_{r-1})^2 - ph_r^2 = (-1)^{r-1}.
\end{equation}

It follows from the second relation above that if $p$ is congruent to 3 modulo 4 then the length $r + 1$ of the period of $\sqrt{p}$ has to be even as otherwise, $-1$ would be a quadratic residue of $p$.

In particular, the period of $\sqrt{p}$ for any prime congruent to 3 modulo 4 has to be even.

We establish an additional recurrence relation that we use later.

**Proposition 2.1.** Let $r + 1$ be the length of the period of $\sqrt{p}$. Then

\begin{equation}
h_r = h_i h_{r-i} + h_{i-1} h_{r-1-i} \quad \text{for} \quad 0 \leq i \leq r - 1.
\end{equation}

**Proof.** By repeated use of the recurrence relation in (2.3), we obtain

\begin{align*}
h_r &= h_0 h_r + h_{-1} h_{r-1}, \quad \text{\hspace{1cm}} \text{(}h_0 = 1, \quad h_{-1} = 0) \\
h_r &= a_r h_{r-1} + h_{r-2} = a_1 h_{r-1} + h_{r-2} = h_1 h_{r-1} + h_0 h_{r-2}, \quad \text{\hspace{1cm}} \text{(}a_j = a_{r+1-j}) \\
h_r &= a_1 h_{r-1} h_{r-2} + h_{r-3} + h_{r-2} = a_1 (a_2 h_{r-2} + h_{r-3}) + h_{r-2} \\
&= (1 + a_1 a_2) h_{r-2} + a_1 h_{r-3} = h_2 h_{r-2} + h_1 h_{r-3}, \\
h_r &= (1 + a_1 a_2) (a_2 h_{r-3} + h_{r-4}) + a_1 h_{r-3}
\end{align*}
\[ = (1 + a_1 a_2)(a_3 h_{r-3} + h_{r-4}) + a_1 h_{r-3} \]
\[ = (a_1 + a_3 + a_1 a_2 a_3) h_{r-3} + (1 + a_1 a_2) h_{r-4} = h_3 h_{r-3} + h_2 h_{r-4}. \]

Continuing in the same fashion, we obtain the desired relation. \[ \square \]

Later, we need the following special case of the above proposition obtained by putting \( i = \frac{r-1}{2} \) when the length \( r + 1 \) of the period of \( \sqrt{p} \) is known to be even:

\[ h_r = h_{r-1} h_{r+1} + h_{r-3} h_{r-1} = h_{r-1} \left( h_{r+1} + h_{r-3} \right). \]

Note that the relation is valid for \( r + 1 = 2 \) as well, with the convention that \( h_{-1} = 0 \).

Next we prove a few other results concerning the convergents of \( \sqrt{p} \). The following lemmas concerning the convergents are used in the subsequent sections.

**Lemma 2.2.** Let \( \frac{k_i}{h_i} \) be the \( i \)-th convergent of the continued fraction of \( \sqrt{p} \) where \( p \) is a prime congruent to 3 modulo 4. Suppose \( r + 1 \) is the length of the period of \( \sqrt{p} \). Then \( h_{\frac{r-1}{2}} \) and \( h_{\frac{r+1}{2}} + h_{\frac{r-3}{2}} \) are co-prime.

**Proof.** As \( p \) is congruent to 3 modulo 4, \( r + 1 \) must be even. Suppose \( d \) is the greatest common divisor of \( h_{\frac{r-1}{2}} \) and \( h_{\frac{r+1}{2}} + h_{\frac{r-3}{2}} \). Then

\[ h_{\frac{r+1}{2}} + h_{\frac{r-3}{2}} - a_{\frac{r+1}{2}} h_{\frac{r-1}{2}} \equiv 0 \mod d. \]

By (2.3) \( h_{\frac{r+1}{2}} = a_{\frac{r+1}{2}} h_{\frac{r-1}{2}} + h_{\frac{r-3}{2}} \), hence

\[ h_{\frac{r+1}{2}} + h_{\frac{r-3}{2}} - a_{\frac{r+1}{2}} h_{\frac{r-1}{2}} = 2h_{\frac{r-3}{2}} \equiv 0 \mod d. \]

By (2.6), \( d \) divides \( h_r = ab \). By proposition 3.1 \( ab \) is odd, hence \( d \) must be odd. It follows from (2.7) that \( d \) must divide \( h_{\frac{r-3}{2}} \. But \( d \) is also a divisor of \( h_{\frac{r-1}{2}} \) and \( h_{\frac{r+1}{2}} + h_{\frac{r-3}{2}} \). Hence \( d \) divides all three consecutive convergents \( h_{\frac{r-1}{2}}, h_{\frac{r+1}{2}} \) and \( h_{\frac{r-3}{2}} \). From the recurrence relation (2.3) of the convergents, it follows that \( d \) divides \( h_{\frac{r-3}{2}}, h_{\frac{r-5}{2}} \) and so on. By going backwards, we can conclude \( d \) divides \( h_2 = 1 + a_1 a_2 \) and \( h_1 = a_1 \), i.e. \( d \) divides 1. \[ \square \]

**Lemma 2.3.** Let \( \frac{k_i}{h_i} \) be the \( i \)-th convergent of \( \langle n; a_1, a_2, \ldots, a_r, 2n \rangle \). Suppose \( r + 1 \) is divisible by 4. Let \( q \) be a prime factor of \( h_r \).

(i) If \( q \mid h_{\frac{r-1}{2}} \), then \( h_{r-1} \equiv 1 \mod q \).

(ii) If \( q \nmid h_{\frac{r-1}{2}} \), then \( h_{r-1} \equiv -1 \mod q \).
Proof (i) Let $q$ be a prime factor of $h_r$ that also divides $h_{r^{-1}}$. By using (2.3) repeatedly, we find that

\[ h_{r^{-1}} = a_{r^{-1}} h_{r^{-2}} + h_{r^{-3}} \equiv h_{r^{-3}} \mod q, \]

\[ h_{r^{-2}} = a_{r^{-2}} h_{r^{-3}} + h_{r^{-4}} + a_{r^{-1} h_{r^{-1}} + h_{r^{-2}}} \equiv a_{r^{-1}} h_{r^{-3}} - h_{r^{-1}} = -h_{r^{-5}} \mod q \]

(2.8) \[ h_{r^{-2}} = a_{r^{-2}} h_{r^{-3}} + h_{r^{-4}} \equiv -a_{r^{-3}} h_{r^{-5}} + h_{r^{-3}} = h_{r^{-2}} \mod q. \]

Note that we are getting the positive sign on the right hand side of the congruence when the index on the left hand side is even. By continuing in this way, we find that

\[ h_{r^{-3}} \equiv h_2 \mod q, \quad h_{r^{-2}} \equiv -h_1 \mod q. \]

It follows from (2.3) that

\[ h_r = a_r h_{r-1} + h_{r-2} = a_1 h_{r-1} + h_{r-2} \equiv h_1 h_{r-1} - h_1 \mod q. \]

Hence $q$ divides $h_1(h_{r-1} - 1)$. If $q$ does not divide $h_1$, we have $h_{r-1} \equiv 1 \mod q$. If $q$ divides $h_1 = a_1$, we still have

\[ h_{r-1} = a_{r-1} h_{r-2} + h_{r-3} \equiv -a_{r-1} h_1 + h_2 \equiv 1 + a_1 a_2 \equiv 1 \mod q. \]

(ii) Let $q$ be a prime factor of $h_r$ that does not divide $h_{r^{-1}}$. By (2.6),

\[ h_{r^{-1}} \equiv -h_{r^{-3}} \mod q. \]

Using (2.3), we now find

(2.9) \[ h_{r^{-1}} = a_{r^{-1}} h_{r^{-2}} + h_{r^{-3}} \equiv -a_{r^{-1}} h_{r^{-3}} + h_{r^{-1}} \equiv h_{r^{-3}} \mod q \]

\[ h_{r^{-2}} = a_{r^{-2}} h_{r^{-3}} + h_{r^{-1}} \equiv a_{r^{-3}} h_{r^{-5}} - h_{r^{-3}} = -h_{r^{-1}} \mod q. \]

Note that we are getting the negative sign in the congruence when the index on the left hand side is even. By continuing in this way, we obtain

\[ h_{r^{-3}} \equiv -h_2 \mod q, \quad h_{r^{-2}} \equiv h_1 \mod q. \]

It follows from (2.3) that

\[ h_r = a_r h_{r-1} + h_{r-2} = a_1 h_{r-1} + h_{r-2} \equiv h_1 h_{r-1} + h_1 \mod q. \]

Hence $q$ divides $h_1(h_{r-1} + 1)$. If $q$ does not divide $h_1$, we have $h_{r-1} \equiv -1 \mod q$. If $q$ divides $h_1 = a_1$, we still have

\[ h_{r-1} = a_{r-1} h_{r-2} + h_{r-3} \equiv a_{r-1} h_1 - h_2 \equiv -1 - a_1 a_2 \equiv -1 \mod q. \]
Lemma 2.4. Let $\frac{k_i}{h_i}$ denote the $i$-th convergent of $\langle n; a_1, a_2, ..., a_r, 2n \rangle$. Suppose $r + 1$ is congruent to 2 modulo 4. Let $q$ be a prime factor of $h_r$.

(i) If $q \mid h_{\frac{r-1}{2}}$, then $h_{r-1} \equiv -1 \mod q$.
(ii) If $q \nmid h_{\frac{r-1}{2}}$, then $h_{r-1} \equiv 1 \mod q$.

Proof. We can use similar arguments as in the previous lemma, noting that the signs in the congruences in (2.8) and (2.9) get interchanged when $r + 1 \equiv 2 \mod 4$. □

3. The fundamental unit of $\mathbb{Q}(\sqrt{p})$

It is well known by Dirichlet’s theorem that the units in the ring of integers of a real quadratic field form an abelian group of rank one, and the smallest unit $> 1$ is referred to as the fundamental unit. Let

$$\xi_p = x + y\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$$

denote the fundamental unit of the real quadratic field $K = \mathbb{Q}(\sqrt{p})$, where $p$ is a prime congruent to 3 modulo 4 as before. The fundamental unit $\xi_p$ is intimately connected with the convergents of $\sqrt{p}$. It is well-known that

$$(3.1) \quad \xi_p = nh_r + h_{r-1} + h_r\sqrt{p}.$$  

The following lemma is crucial for our subsequent work (cf. lemma 3.1 in [3]).

Proposition 3.1. Let $p$ be a prime congruent to 3 modulo 4, and $\xi_p = x + y\sqrt{p}$ be the fundamental unit of $\mathbb{Q}(\sqrt{p})$. We have $2x = a^2 + pb^2$ and $y = ab$ for some relatively prime, odd integers $a$ and $b$. Moreover $a^2 - pb^2 = \pm 2$, where the sign is positive if and only if $p$ is congruent to 7 modulo 8.

As 2 ramifies in the extension $K$, $2\mathcal{O}_K = p^2$. It is well known that $\mathbb{Q}(\sqrt{p})$ had odd class number when $p$ is a prime congruent to 3 mod 4. Since the ideal class of $p$ has order dividing 2, $p$ has to be a principal ideal. Therefore, there exist integers $a$, $b$ and $j$ such that

$$(3.2) \quad 2\xi_p^j = (a + b\sqrt{p})^2.$$  

If $j$ were even, (3.2) would imply that $\sqrt{p} \in \mathbb{Q}(\sqrt{p})$. Hence $j$ has to be odd, and we can take $j = 1$ (in 2.3) by absorbing the even powers of the unit $\xi_p$ on the right hand side. Thus,

$$(3.3) \quad 2\xi_p = (a + b\sqrt{p})^2 \implies 2x = a^2 + pb^2, \quad y = ab.$$
As \( \xi_p = x + y\sqrt{p} \) is a unit, \( a \) and \( b \) have to be coprime. As \( a^2 + pb^2 = 2x \) is even, \( a \) and \( b \) must have same parity and hence both must be odd.

As \( -1 \) is not a quadratic residue of \( p \), the norm of \( \xi_p \) can not be \(-1\), i.e.,

\[
N_{K/Q}(\xi_p) = x^2 - py^2 = 1.
\]

Substituting \( x \) and \( y \) from (3.3), we obtain

\[
\left( \frac{a^2 + pb^2}{2} \right)^2 - pa^2b^2 = 1 \implies a^2 - pb^2 = \pm 2.
\]

When \( p \equiv 7 \mod 8 \), \(-2\) is not a quadratic residue of \( p \) and hence

\[
a^2 - pb^2 = 2.
\]

When \( p \equiv 3 \mod 8 \), \( 2 \) is not a quadratic residue of \( p \) and hence

\[
a^2 - pb^2 = -2. \quad \square
\]

The following corollaries of proposition 3.1 are used later.

**Corollary 3.2.** Let \( p \) be a prime congruent to 7 modulo 8 and \( q \) be any prime factor of \( h_r \).

Then,

(i) \( h_{r-1} \equiv -1 \mod q \iff q \mid a \).

(ii) \( h_{r-1} \equiv 1 \mod q \iff q \mid b \).

**Proof.** As \( p \equiv 7 \mod 8 \), (3.3), (3.4) and (3.5) imply that

\[
y = h_r = ab, \quad x + 1 = nh_r + h_{r-1} + 1 = a^2, \quad x - 1 = nh_r + h_{r-1} - 1 = pb^2.
\]

If \( q \) is a prime dividing \( h_r = ab \), it has to be odd as both \( a \) and \( b \) are odd by proposition 3.1. By (3.7), \( h_{r-1} \equiv -1 \mod q \) is equivalent to \( a^2 \equiv 0 \mod q \). If \( q \) divides \( b \), it is evident from (3.7) that \( h_{r-1} \equiv 1 \mod q \). If \( h_{r-1} \equiv 1 \mod q \), then \( pb^2 \equiv 0 \mod q \) by (3.7). Also, \( q \mid ab = h_r \). If \( q \) does not divide \( b \), \( q \) has to divide \( p \) as well as \( a \), which would contradict \( a^2 - pb^2 = 2 \) as \( q \) is odd. Therefore \( q \) must divide \( b \). \( \square \)

**Corollary 3.3.** Let \( p \) be a prime congruent to 3 modulo 8 and \( q \) be any prime factor of \( h_r \).

Then,

(i) \( h_{r-1} \equiv 1 \mod q \iff q \mid a \).

(ii) \( h_{r-1} \equiv -1 \mod q \iff q \mid b \).
Proof. As \( p \equiv 3 \mod 8 \), (3.1), (3.3) and (3.6) imply that

\[
y = h_r = ab, \quad x - 1 = nh_r + h_{r-1} - 1 = a^2, \\
x + 1 = nh_r + h_{r-1} + 1 = pb^2
\]

(3.8)

The corollary follows by a similar argument as in the previous corollary. \( \Box \)

4. Length of the period of \( \sqrt{p} \)

Our main objective is to express the parameters \( a \) and \( b \) of the fundamental unit of \( \mathbb{Q}(\sqrt{p}) \) in terms of the convergents of \( \sqrt{p} \). As \( a \) and \( b \) satisfy \( a^2 - pb^2 = \pm 2 \), we would then obtain explicit solutions for the equation \( u^2 - pv^2 = \pm 2 \). But our approach also yields a few interesting results concerning the continued fraction of \( \sqrt{p} \). We include these results as proposition 4.1 and corollaries 6.1, 6.2.

Proposition 4.1. Let \( p \) be a prime congruent to 3 modulo 4. Then the length of the period of the continued fraction of \( \sqrt{p} \) is divisible by 4 if \( p \) is congruent to 7 modulo 8 and is of the form \( 4k + 2 \) if \( p \) is congruent to 3 modulo 8.

We show that if above corollary does not hold, then the parameters \( a \) and \( b \) can be associated to the convergents of \( \sqrt{p} \) by lemmas 4.2 and 4.3 which lead to a contradiction. Later, proposition 4.1 allows us to relate \( a \) and \( b \) with the correct convergents of \( \sqrt{p} \) via proposition 5.1 in the next section.

Lemma 4.2. Let \( p \) be a prime congruent to 7 modulo 8 such that the continued fraction of \( \sqrt{p} \) has period of length \( r + 1 \equiv 2 \) modulo 4. Then \( b = h_{r+1} \frac{1}{2} + h_{r-1} \frac{1}{2} \) and \( a = h_{r+1} \frac{1}{2} \).

Proof. We show that \( h_{r+1} \frac{1}{2} \) divides \( a \) and \( a \) divides \( h_{r+1} \frac{1}{2} \). First, let \( q \) be a prime factor of \( h_{r+1} \frac{1}{2} \). By lemma 2.4 \( h_{r+1} \frac{1}{2} \equiv -1 \mod q \). By corollary 3.2 \( q \mid a \). But \( h_{r+1} \frac{1}{2} \) divides \( h_r = ab \) by (2.6), and \( a \) and \( b \) are coprime by proposition 3.1. It follows that \( h_{r+1} \frac{1}{2} \) divides \( a \). If \( q \) is a prime factor of \( a \), then by corollary 3.2 \( h_{r-1} \equiv -1 \mod q \) and by lemma 2.4 \( q \) is a factor of \( h_{r-1} \). As \( ab = h_{r+1} \frac{1}{2} (h_{r+1} \frac{1}{2} + h_{r-1} \frac{1}{2}) \) where the factors on the same side are coprime, we have \( a = h_{r+1} \frac{1}{2} \) and therefore \( b = h_{r+1} \frac{1}{2} + h_{r-1} \frac{1}{2} \).

Lemma 4.3. Let \( p \) be a prime congruent to 3 modulo 8 such that the continued fraction of \( \sqrt{p} \) has period of length \( r + 1 \equiv 0 \) modulo 4. Then \( b = h_{r+1} \frac{1}{2} + h_{r-1} \frac{1}{2} \) and \( a = h_{r+1} \frac{1}{2} \).
SOLUTIONS FOR $u^2 - pv^2 = \pm 2$ AND MORDELL’S CONJECTURE

Proof. If possible, let $r + 1 \equiv 0 \mod 4$. Let $q$ be a prime factor of $h_{\frac{r+1}{2}}$. By lemma 2.3, $h_{\frac{r-1}{2}} \equiv 1 \mod q$. By corollary 3.3, $q \mid a$. As $a$ and $b$ are coprime, it implies that $h_{\frac{r-1}{2}}$ divides $a$. If $q$ is a prime factor of $a$, then by corollary 3.3, $h_{\frac{r-1}{2}} \equiv 1 \mod q$ and by lemma 2.3, $q$ is a factor of $h_{\frac{r-1}{2}}$. As $ab = h_{\frac{r-1}{2}}(h_{\frac{r+1}{2}} + h_{\frac{r-3}{2}})$ where the factors on the same side are coprime, we have $a = h_{\frac{r-1}{2}}$ and therefore $b = h_{\frac{r+1}{2}} + h_{\frac{r-3}{2}}$. □

Proof of proposition 4.1 If possible, let $p$ be a prime congruent to 7 mod 8 such that the continued fraction of $\sqrt{p}$ has period of length $r + 1 \equiv 2$ modulo 4. Noting that $h_{\frac{r+1}{2}} = a_{\frac{r+1}{2}}h_{\frac{r-1}{2}} + h_{\frac{r-3}{2}}$, we can deduce from lemma 4.2 that

$$a^2 - pb^2 = a^2(1 - pa_{\frac{r+1}{2}}) - 4ph_{\frac{r+1}{2}}h_{\frac{r-3}{2}} < 2,$$

which is not possible by (3.5). It follows that $r + 1 \equiv 0 \mod 4$ if $p \equiv 7 \mod 8$.

Similarly, if $p$ is congruent to 3 mod 8 such that $r + 1 \equiv 0$ modulo 4, then by lemma 4.3 and by same reasoning as (4.1), we obtain

$$a^2 - pb^2 = a^2(1 - pa_{\frac{r+1}{2}}) - 4ph_{\frac{r+1}{2}}h_{\frac{r-3}{2}} < -2,$$

which contradicts (3.6). □

5. Solution of $u^2 - pv^2 = \pm 2$ in terms of convergents

Proposition 5.1. Let $p$ be a prime congruent to 3 modulo 4 and

$$\xi_p = x + y\sqrt{p} = \frac{a^2 + pb^2}{2} + ab\sqrt{p}$$

be the fundamental unit of $\mathbb{Q}(\sqrt{p})$ as in proposition 3.1. Then $b = h_{\frac{r-1}{2}}$ and $a = h_{\frac{r+1}{2}} + h_{\frac{r-3}{2}}$.

Proof. We show that $b$ divides $h_{\frac{r-1}{2}}$ and vice versa. First consider the case $p \equiv 7 \mod 8$, so $r + 1 \equiv 0$ modulo 4 by proposition 4.1.

Let $q$ be a prime that divides $h_{\frac{r-1}{2}}$. By lemma 2.3, $h_{\frac{r-1}{2}} \equiv 1 \mod q$, and by corollary 3.2, $q$ divides $b$. As $a$ and $b$ are coprime, it implies that $h_{\frac{r-1}{2}}$ divides $b$. Conversely, let $q$ be a prime that divides $b$. By corollary 3.2, $h_{\frac{r-1}{2}} \equiv 1 \mod q$, hence by lemma 2.3, $q$ divides $h_{\frac{r-1}{2}}$. As
\[ ab = h_{r+1} (h_{r+1} + h_{r-3}) \] where the factors on the same side are coprime, we have \( b \) divides \( h_{r+1} \). Therefore \( b = h_{r+1} \) and \( a = h_{r+1} + h_{r-3} \).

Next we consider \( p \equiv 3 \) mod 8. Then \( r + 1 \equiv 2 \) mod 4 by proposition \[ \text{Proposition 4.1} \]. By using corollary \[ \text{Corollary 3.3} \] and lemma \[ \text{Lemma 2.4} \] as above, we arrive at the conclusion in this case too. \( \square \)

The main theorem of the article can be stated as follows.

**Theorem 5.2.** Let \( p \) be a prime congruent to 3 modulo 4. Let \( r + 1 \) be the length of the period of the continued fraction of \( \sqrt{p} \) and \( \frac{h_i}{m_i} \) denote the \( i \)-th convergent of the continued fraction of \( \sqrt{p} \). Then \( u = h_{r+1} + h_{r-3} \) and \( v = h_{r+1} \) satisfy \( u^2 - pv^2 = 2 \) when \( p \equiv 7 \) mod 8 and \( u^2 - pv^2 = -2 \) when \( p \equiv 3 \) mod 8.

**Proof.** By proposition \[ \text{Proposition 5.1} \] we know that \( a = h_{r+1} + h_{r-3} \) and \( b = h_{r-1} \). By proposition \[ \text{Proposition 3.1} \] we know that \( a^2 - pb^2 = 2 \) when \( p \equiv 7 \) mod 8 and \( a^2 - pb^2 = -2 \) when \( p \equiv 3 \) mod 8. Therefore, we obtain explicit solutions for the equation \( u^2 - pv^2 = \pm 2 \) in terms of the convergents for \( \sqrt{p} \) as stated in the theorem. \( \square \)

6. **The central term \( a_{\frac{r+1}{2}} \)**

In this section, we prove certain results concerning the central term \( a_{\frac{r+1}{2}} \) in the palindrome \( a_1, a_2, \ldots, a_r \) of the period \( a_1, a_2, \ldots, a_r, 2n \) of the continued fraction of \( \sqrt{p} \) as a corollary of proposition \[ \text{Proposition 5.1} \]. In fact we were initially not aware that the result was previously known by work Gebulova in \[ \text{[7]} \], and we thank Prof. Y. Kishi and Prof. M. Waldschmidt for pointing it out to us.

**Corollary 6.1.** The central term \( a_{\frac{r+1}{2}} \) in the of the palindromic part of the period of the continued fraction of \( \sqrt{p} \) is always odd for any prime \( p \) congruent to 3 modulo 4.

**Proof.** Let \( p \) be a prime congruent to 3 mod 4. By \[ \text{Lemma 2.3} \] and proposition \[ \text{Proposition 5.1} \]

\[
\frac{h_{r+1}}{2} - h_{r-3} = a_{\frac{r+1}{2}} h_{r+1} = \frac{a_{\frac{r+1}{2}} b}{2},
\]

\[
\frac{h_{r+1}}{2} + h_{r-3} = a,
\]

\[
\implies 2h_{\frac{r+1}{2}} = a + \frac{a_{\frac{r+1}{2}} b}{2}.
\]

Since both \( a \) and \( b \) are odd, \( a_{\frac{r+1}{2}} \) has to be odd as the left hand side is even. \( \square \)
Corollary 6.2. For any prime $p$ congruent to 3 modulo 4, the central term $a_{\frac{r+1}{2}}$ in the palindromic part of the period of the continued fraction of $\sqrt{p}$ is either $n = \lfloor \sqrt{p} \rfloor$ or $n - 1$ depending on whichever is odd.

Before proving corollary 6.2, we show an useful upper bound for $a_{\frac{r+1}{2}}$ as follows.

Lemma 6.3. Suppose $p$ is a prime congruent to 3 modulo 4 and

$$\sqrt{p} = \langle n; a_1, a_2, \ldots, a_{\frac{r+1}{2}}, \ldots, a_r, 2n \rangle.$$ 

Then $a_{\frac{r+1}{2}} < \sqrt{p}$.

Proof. If possible, let $a_{\frac{r+1}{2}} \geq \sqrt{p}$. Then $a_{\frac{r+1}{2}} \geq n + 1$ where $\lfloor \sqrt{p} \rfloor = n$. By proposition 5.1 and (2.3), we have

$$a = h_{\frac{r+1}{2}} + h_{\frac{r-3}{2}} = a_{\frac{r+1}{2}} h_{\frac{r-1}{2}} + h_{\frac{r-3}{2}} \geq (n+1)b + 2$$

(6.1)

$$\implies a^2 > (n+1)^2b^2 + 4 > pb^2 + 2.$$ 

But the last inequality contradicts proposition 3.1, which asserts that $a^2 - pb^2 = \pm 2$. Note that when $r + 1 = 2$, we have $h_{\frac{r-3}{2}} = h_{\frac{r-1}{2}} = 0$ in (6.1). But even in that case too we still would have $a^2 \geq (n+1)^2b^2 > pb^2 > pb^2 - 2$ which contradicts the equality $a^2 - pb^2 = -2$ of proposition 3.1. Therefore, we must have $a_{\frac{r+1}{2}} < \sqrt{p}$. □

Proof of corollary 6.2: We want to prove that $a_{\frac{r+1}{2}} = n$ or $n - 1$. By the previous lemma, $a_{\frac{r+1}{2}} < \sqrt{p}$. If possible, suppose $a_{\frac{r+1}{2}} \leq \sqrt{p} - 2$. By proposition 5.1,

$$a = h_{\frac{r+1}{2}} + h_{\frac{r-3}{2}} < h_{\frac{r+1}{2}} + h_{\frac{r-1}{2}} = h_{\frac{r+1}{2}} + b,$$

$-p \leq -a_{\frac{r+1}{2}}^2 - 4a_{\frac{r+1}{2}} - 4$ (assuming $\sqrt{p} \geq a_{\frac{r+1}{2}} + 2$),

$$\implies a^2 - pb^2 < h_{\frac{r+1}{2}}^2 + 2bh_{\frac{r+1}{2}} + b^2 - pb^2$$

$$< (a_{\frac{r+1}{2}} h_{\frac{r-1}{2}} + h_{\frac{r-3}{2}})^2 + 2bh_{\frac{r+1}{2}} + b^2 - pb^2$$

$$< (a_{\frac{r+1}{2}} b^2 + 2a_{\frac{r+1}{2}} bh_{\frac{r-3}{2}} + h_{\frac{r-3}{2}}^2) + 2bh_{\frac{r+1}{2}} + b^2$$

$$- (a_{\frac{r+1}{2}} + 4a_{\frac{r+1}{2}} + 4)b^2$$ (as $b = h_{\frac{r-1}{2}}$ by prop 5.1)

$$< 2a_{\frac{r+1}{2}} b^2 + b^2 + 2bh_{\frac{r+1}{2}} + b^2 - 4a_{\frac{r+1}{2}} b^2 - 4b^2$$

$$= -2b^2 + 2bh_{\frac{r+1}{2}} - 2a_{\frac{r+1}{2}} b^2 = -2b^2 + 2b(h_{\frac{r+1}{2}} - a_{\frac{r+1}{2}} b)$$

$$= -2b^2 + 2bh_{\frac{r-3}{2}}$$ (by 2.3)

$$\implies a^2 - pb^2 < -2b(b - h_{\frac{r-3}{2}}) \leq -2$$ (since $h_{\frac{r-3}{2}} < h_{\frac{r-1}{2}} = b$).
But the final inequality above contradicts proposition 3.1 which asserts that \( a^2 - pb^2 = \pm 2 \). Therefore, we must have

\[
\sqrt{p} - 2 < a_{\frac{r+1}{2}} < \sqrt{p},
\]

and \( a_{\frac{r+1}{2}} \) is either \( n \) or \( n - 1 \). Applying corollary 6.1, \( a_{\frac{r+1}{2}} \) is either \( n \) or \( n - 1 \) depending on whichever is odd. \( \square \)

7. Families of \( p \) satisfying Mordell’s Conjecture

In this section, we discuss certain applications of our results. It is easy to see that the continued fraction of \( \sqrt{(n+1)^2 - 2} \) has period of length 4, or more precisely,

\[
(7.1) \quad \sqrt{(n+1)^2 - 2} = \langle n; 1, n - 1, 1, 2n \rangle \quad \text{for any natural number } n \geq 2.
\]

We show that the converse holds for any prime \( p \) with continued fraction of \( \sqrt{p} \) having period of length 4.

**Proposition 7.1.** Any prime \( p \) with \( \sqrt{p} \) having periodic continued fraction of length 4 must be of the form \( (n+1)^2 - 2 \), where \( n = \lfloor \sqrt{p} \rfloor \).

**Proof.** Suppose \( p \) is a prime number with \( \sqrt{p} = \langle n; \alpha, \beta, \alpha, 2n \rangle \). By (2.4) and (2.5),

\[
(7.2) \quad k_3^2 - ph_3^2 = 1 \implies p = \frac{k_3^2 - 1}{h_3^2},
\]

where

\[
\frac{k_3}{h_3} = n + \frac{1}{\alpha + \frac{1}{\beta + \frac{1}{\alpha}}} = \frac{n\alpha^2 \beta + 2n\alpha + \alpha \beta + 1}{\alpha^2 \beta + 2\alpha}.
\]

By corollaries 6.1 and 6.2, \( \beta \) is either \( n = \lfloor \sqrt{p} \rfloor \) or \( n - 1 \) depending on whichever is odd. First we show that \( n \) must be even and \( \beta = n - 1 \) for such a prime.

If possible, let \( n \) be odd. Then \( \beta = n \) by corollaries 6.1 and 6.2. By (7.2),

\[
p = n^2 + \frac{n(2n\alpha + 3)}{\alpha(n\alpha + 2)}.
\]

But \( n\alpha + 2 \) is coprime to \( 2n\alpha + 3 \), as any common factor of \( n\alpha + 2 \) and \( 2n\alpha + 3 \) has to divide \( 2(n\alpha + 2) - (2n\alpha + 3) = 1 \). Therefore, \( n\alpha + 2 \) has to divide \( n \), which is not possible.

Hence \( \lfloor \sqrt{p} \rfloor = n \) is even, and \( \beta = n - 1 \) by corollaries 6.1 and 6.2. By (7.2),

\[
(7.3) \quad p = n^2 + \frac{2n^2\alpha + 3n - 2n\alpha - 1}{n\alpha^2 - \alpha^2 + 2\alpha}.
\]
As \( p \) is an integer, we must have

\[
2n^2\alpha + 3n - 2n\alpha - 1 \equiv 0 \pmod{na^2 - \alpha^2 + 2\alpha}
\]

\[
\implies 2n(na^2 - \alpha^2 + 2\alpha) - (n\alpha + \alpha) \equiv 0 \pmod{na^2 - \alpha^2 + 2\alpha}.
\]

It follows that \( na^2 - \alpha^2 + 2\alpha \) divides \( n\alpha + \alpha \), which is only possible if \( \alpha = 1 \). By (7.3), we now have \( p = n^2 + 2n - 1 = (n + 1)^2 - 2 \).

\[\square\]

**Proposition 7.2.** Any prime \( p \) such that \( \sqrt{p} \) has a period of length 2 must be of the form \( p = n^2 + 2 \) where \( n \) is odd.

**Proof.** Let \( \sqrt{p} = (n; \overline{n\beta}) \) where \( n = |p| \). Then

\[
\frac{k_1}{h_1} = n + \frac{1}{\beta} = \frac{n\beta + 1}{\beta},
\]

and \( k_1^2 - ph_1^2 = 1 \implies p = \frac{k_1^2 - 1^2}{h_1} = \frac{n^2\beta^2 + 2n\beta}{\beta^2} = \frac{n(n\beta + 2)}{\beta}.
\]

If \( d = \gcd(\beta, n\beta + 2) \) then \( d \mid 2 \). But by our results \( \beta \) is odd, hence \( d = 1 \). Therefore, \( \beta \mid n \), but \( \beta = n \) or \( n - 1 \) by our results on the central term. Hence \( \beta = n \) and \( p = \frac{(n^2 + 1)^2 - 1}{n^2} = n^2 + 2 \), where \( n \) is odd.

\[\square\]

As a consequence of our results, we can also ascertain that the conjecture of Mordell on the fundamental unit of \( \mathbb{Q}(\sqrt{p}) \) holds when the continued fraction of \( \sqrt{p} \) has period of length 2, 4 or 6.

**Corollary 7.3.** Let \( x + y\sqrt{p} \) be the fundamental unit of \( \mathbb{Q}(\sqrt{p}) \), where \( p \) is a prime with \( \sqrt{p} \) having continued fraction of period of length 2. Then \( p \) does not divide \( y \).

**Proof.** If \( p \) divides \( y \) then it is clear from (3.2) that \( p \) has to divide \( b \), where \( b \) is as given in proposition (3.1). However, \( b = h_{-1} = h_0 \) by proposition (5.1). But \( h_0 = 1 \) and hence \( p \) can not divide \( y \).

\[\square\]

**Corollary 7.4.** Let \( x + y\sqrt{p} \) be the fundamental unit of \( \mathbb{Q}(\sqrt{p}) \), where \( p \) is a prime with \( \sqrt{p} \) having continued fraction of period 4. Then \( p \) does not divide \( y \).

**Proof.** If \( p \) divides \( y \) then it is clear from (3.2) that \( p \) has to divide \( b \), where \( b \) is as given in proposition (3.1). However, \( b = h_{-1} = h_1 \) by proposition (5.1). By corollary (7.1) and (7.3), we have \( h_1 = 1 \) and hence \( p \) can not divide \( y \).

\[\square\]
Corollary 7.5. Let $x + y\sqrt{p}$ be the fundamental unit of $\mathbb{Q}(\sqrt{p})$, where $p$ is a prime with $\sqrt{p} = \langle n; \alpha, \beta, \gamma, \delta, \alpha, 2n \rangle$. Then $p$ does not divide $y$.

Proof. We first show that $\alpha\beta < 2n$. We have

$$p = n^2 + t, \quad t \leq 2n \text{ and } \sqrt{p} = n + \frac{1}{t + \frac{1}{2n + \sqrt{p} - n}}, \quad 0 < \sqrt{p} - n < 1.$$ 

Now, the coefficient $\alpha$ in the continued fraction of $\sqrt{p}$ is given by

$$2n = t\alpha + r_1, \quad 0 < r_1 < t.$$

Note that $r_1 = 0$ would imply that $\sqrt{p} = \langle n; \alpha, 2n \rangle$. Now,

$$\sqrt{p} = n + \frac{1}{t + \frac{1}{2n + \sqrt{p} - n}} = n + \frac{1}{\alpha + \frac{1}{t + \frac{1}{2n + \sqrt{p} - n} - 1}}.$$

We observe that

$$p - (n - r_1)^2 = (p - n^2) + 2nr_1 - r_1^2 = t + (t\alpha + r_1)r_1 - r_1^2 = t(1 + \alpha r_1),$$

$$t(\sqrt{p} + (n - r_1)) = t(2n - r_1 + \sqrt{p} - n).$$

It follows that the next coefficient $\beta$ in the continued fraction of $\sqrt{p}$ is given by

$$2n - r_1 = (1 + \alpha r_1)\beta + r_2, \quad 0 < r_2 < 1 + \alpha r_1.$$

As $r_1 \geq 1$, we can conclude from the last equality that $\alpha\beta < 2n$.

Now, by proposition 5.1

$$b = h_{r-1} = h_2 = \alpha \beta + 1 \leq 2n < p.$$

Hence $p$ can not divide $b$, and therefore it can not divide $y$ by (3.2). \qed

By the conjecture of P. Chowla and S. Chowla mentioned in the introduction, there exist infinitely many primes $p$ such that $\sqrt{p}$ has period of length $k$ for any natural number $k$. Their conjecture remained unproven, though Friesen ([6]) has shown the existence of infinitely many square-free integers $N$ such that $\sqrt{N}$ has period of length $k$ for any natural number $k$. By corollaries 7.3, 7.4 and 7.5, we thus obtain three conjecturally infinite families of primes for which Mordell’s Conjecture holds. The existence of infinitely many primes $p$ with $\sqrt{p}$ having continued fraction of period of length 2 and of length 4 is predicted by Bunyakovsky’s conjecture as well. Bunyakovsky’s conjecture states that if $f(x)$ is an irreducible polynomial in $\mathbb{Z}[x]$ with positive leading coefficient such that $gcd\{f(n) | n \in \mathbb{N}\} = 1$ then $f(n)$ takes infinitely many prime values as $n$ runs over natural numbers. The polynomials $x^2 + 2$ and $(x + 1)^2 - 2$ clearly satisfies those conditions. In view of propositions 7.1 and 7.2 each of the
two families of primes \( p \) such that \( \sqrt{p} \) has period of length 2 or 4 is infinite by Bunyakovosky’s Conjecture as well.

As the conjecture of Mordell has been verified for all primes \( p < 10^7 \) \([2]\), we provide a few examples of primes \( p > 10^7 \) that satisfy the conjecture by using proposition \([7,4]\) and corollary \([7,4]\).

\[
\begin{array}{|c|c|c|}
\hline
p &=& (n + 1)^2 - 2 \quad \sqrt{p} = (n, 1, n - 1, 1, 2n) \quad \xi_p = x + y\sqrt{p} \\
10017223 &=& (3164, 1, 3163, 1, 6328) \quad 10017224 + 3165\sqrt{10017223} \\
20948927 &=& (4576, 1, 4575, 1, 9152) \quad 20948928 + 4577\sqrt{20948927} \\
21003887 &=& (4582, 1, 4581, 1, 9164) \quad 21003888 + 4583\sqrt{21003887} \\
21022223 &=& (4584, 1, 4583, 1, 9168) \quad 21022224 + 4585\sqrt{21022223} \\
\hline
\end{array}
\]

References

[1] N. C. Ankeny, E. Artin and S. Chowla; The class-number of real quadratic fields; Ann. of Math.; 56 (1952), 479–493.

[2] B. D. Beach, H. C. Williams and C. R. Zarnke; Some computer results on units in quadratic and cubic fields, Proc. 25th Summer Meeting Can. Math. Congress, Lakehead Univ. (1971), 609–648.

[3] D. Chakraborty, and A. Saikia; Congruence relations for the fundamental unit of a pure cubic field and its class number; Journal of Number Theory; 166 (2016), 76–84.

[4] P. Chowla and S. Chowla; Problems on periodic simple continued fractions, Proc. Nat. Acad. Sci. U.S.A. 69 (1972), 3745.

[5] H. Davenport; Higher Arithmetic, Cambridge University Press (2008).

[6] C. Friesen, On continued fractions of given period, Proc. Amer. Math. Soc. 103 (1988), no. 1, 9–14.

[7] E.P. Golubeva; Class numbers of real quadratic fields of discriminant \( 4p \). (Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) 204 (1993), Anal. Teor. Chisell i Teor. Funktsii, 11, 11–36, 167.

[8] F. Lemmermeyer; Higher descent on Pell Conics I. From Legendre to Selmer arXiv:math/0311308v1, 2003.

[9] L. J. Mordell, On a Pellian equation conjecture, Acta Arith. 6 (1960), 137–144.

[10] L. J. Mordell, On a Pellian equation conjecture II, Journal of London Math. Soc. 36 (1961), 282–288.

[11] A. J. Van Der Poorten, H. J. J. te Riele and H. C. Williams; Computer verification of the Ankeny-Artin-Chowla conjecture for all primes less than \( 100000000000 \); Math. Comp. 70 (2001), 1311–1328.

Department of Mathematics, Tezpur University, Tezpur, Assam, India

E-mail address: debopam@tezu.ernet.in

Department of Mathematics, Indian Institute of Technology Guwahati, Guwahati, India

E-mail address: a.saikia@iitg.ac.in