THE ORDER OF THE FUNDAMENTAL SOLUTION OF $X^2 - DY^2 = 1$ IN $\mathbb{Z}[^{\sqrt{D}}]/(D)$

Stephen Choi  
Department of Mathematics, Simon Fraser University, Burnaby, British Columbia, Canada  
schola@sfu.ca

Daniel Tarnu  
Department of Mathematics, Simon Fraser University, Burnaby, British Columbia, Canada  
daniel_tarnu@sfu.ca

Received: 7/1/22, Accepted: 8/17/22, Published: 8/24/22

Abstract

Let $D$ be a positive integer that is not a perfect square and $x_0 + y_0 \sqrt{D}$ be the fundamental solution of Pell’s equation $x^2 - Dy^2 = 1$. In this article, we study the multiplicative order of the fundamental solution in $\mathbb{Z}[^{\sqrt{D}}]/(D)$, which we denote by $g(D)$. Ultimately, we describe the fundamental solution of $x^2 - D^{2\ell+1}y^2 = 1$ in terms of $x_0$ and $y_0$ for $\ell \geq 0$, and use this to conclude that

$$g(D^{2\ell+1}) = \begin{cases} 
D^{2\ell+1} & \text{if order}(x_0, D) = 1 \text{ and } D \text{ is odd}, \\
2D^{2\ell+1} & \text{if order}(x_0, D) = 2 \text{ and } D \text{ is odd}, \\
D^{2\ell+1} & \text{if } D \text{ is even}
\end{cases}$$

for sufficiently large $\ell$.

1. Introduction

Consider Pell’s equation

$$x^2 - Dy^2 = 1 \quad (1.1)$$

where $D$ is a positive integer that is not a perfect square. We consider the ring

$$\mathbb{Z}[\sqrt{D}] := \{x + y\sqrt{D} : x, y \in \mathbb{Z}\}.$$ 

We say that $s + t\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$ or $(s, t) \in \mathbb{Z}^2$ is an integer solution (or simply solution) of Equation (1.1) if $s^2 - Dt^2 = 1$. Let $x_0 + y_0 \sqrt{D}$ be the fundamental solution of Pell’s Equation (1.1), i.e., $x_0 + y_0 \sqrt{D}$ is the smallest positive solution of
Equation (1.1). It is well-known that all the solutions of Equation (1.1) are given by
\[ \{ \pm (x_0 \pm y_0 \sqrt{D})^\ell : \ell \in \mathbb{Z} \}. \]

Let \( m \geq 2 \) and \( \Phi_m \) be the reduction map from \( \mathbb{Z}[\sqrt{D}] \) to \( \mathbb{Z}[\sqrt{D}]/(m) \) such that
\[ \Phi_m(x + y\sqrt{D}) = \overline{x} + \overline{y}\sqrt{D} \]
where \( \overline{x} \equiv x \pmod{m} \) and \( \overline{x} \in \{0, 1, \ldots, m-1\} \) and similarly with \( \overline{y} \).

Since \( (x_0 + y_0\sqrt{D})(x_0 - y_0\sqrt{D}) = x_0^2 - Dy_0^2 = 1 \)
we have \( (x_0 + y_0\sqrt{D})(x_0 - y_0\sqrt{D}) = 1 \) in \( \mathbb{Z}[\sqrt{D}]/(m) \). Hence \( \Phi_m(x_0 + y_0\sqrt{D}) \) is a unit in the finite ring \( \mathbb{Z}[\sqrt{D}]/(m) \). We call \( g_D(m) \) the multiplicative order of \( \Phi_m(x_0 + y_0\sqrt{D}) \) in the unit ring of \( \mathbb{Z}[\sqrt{D}]/(m) \). In this article, we are interested in studying \( g_m(D) \) in the case that \( m = D \) and denote \( g_D(D) \) by \( g(D) \). We will study and obtain an explicit formula for \( g(D) \).

The authors believe there is little literature on this notion of order besides [6]. In [6], Chahal and Priddis study the order of \( \Phi_m(G) \) in \( \text{GL}_2(\mathbb{Z}/m\mathbb{Z}) \) where \( G \) is the solution set for \( x^2 - Dy^2 = 1 \) realized as a group of 2 \( \times \) 2 matrices with integer entries. Their order is more general than ours. We only consider the special case that \( m = D \).

The order \( g_m(D) \) has some applications. In [8], we use \( g_k(2A) \) to find infinitely many solutions \( (s,t) \in \mathbb{N}^2 \) of \( x^2 - ky^2 = 1 \) with \( s + t \equiv 1 \pmod{2A} \) and \( s + kt \equiv 1 \pmod{2A} \) where \( A \in \mathbb{N} \). This step is essential in the proof of the main theorem in [8]. The order \( g(D) \) is also useful in finding all solutions \( (x,y) \) of the generalized Pell equation
\[ x^2 - Dy^2 = k \]
satisfying the congruence conditions
\[ x \equiv a \pmod{D} \quad \text{and} \quad y \equiv b \pmod{D} \]
where \( \text{gcd}(D,k) = 1 \). If \( u := x_0 + y_0\sqrt{D} \) is the fundamental solution of \( x^2 - Dy^2 = 1 \), then it is well-known that every solution \( (x, y) \) of Equation (1.2) is in the form of
\[ x + y\sqrt{D} = \pm(x' + y'\sqrt{D})(x_0 + y_0\sqrt{D})^\ell, \]
for \( \ell \in \mathbb{Z} \) and some solution \( (x', y') \) of Equation (1.2) satisfying
\[ |x'| \leq \frac{\sqrt{|k|}(\sqrt{u} + 1)}{2}, \quad |y'| \leq \frac{\sqrt{|k|}(\sqrt{u} + 1)}{2\sqrt{D}}. \]
We then find all of the finitely many solutions \( (x_i, y_i), 1 \leq i \leq q \), of Equation (1.2) satisfying Equation (1.3) and Equation (1.4). If no such \( (x_i, y_i) \) exist, then Equation (1.2) has no solution satisfying the congruence conditions Equation (1.3) as we show below.
Proposition 1. Let $x_i + y_i \sqrt{D}, 1 \leq i \leq q$, be the solutions of Equation (1.2) satisfying Equation (1.3) and Equation (1.4). The solutions of of the generalized Pell Equation (1.2) satisfying Equation (1.3) are

$$\pm (x_i \pm y_i \sqrt{D})(x_0 \pm y_0 \sqrt{D})^{ng(D)}, n \in \mathbb{Z}, 1 \leq i \leq q.$$ 

Proof. If $(x, y)$ is a solution of Equation (1.2), we have $\gcd(x, D) = 1$ because $\gcd(k, D) = 1$. Note that if $x + y \sqrt{D} = (x' + y' \sqrt{D})(s + t \sqrt{D}) = (x's + y'tD) + (y's + x't)\sqrt{D}$ (1.5) then

$$\begin{cases} x \equiv x' \pmod{D}, \\ y \equiv y' \pmod{D}, \quad \text{if and only if} \quad \begin{cases} s \equiv 1 \pmod{D}, \\ t \equiv 0 \pmod{D}. \end{cases} \end{cases}$$

Indeed, if $s \equiv 1 \pmod{D}$ and $t \equiv 0 \pmod{D}$, then from Equation (1.5), we have $x \equiv x's \equiv x' \pmod{D}$ and $y \equiv y's \equiv y' \pmod{D}$. Conversely, if $x \equiv x' \pmod{D}$ and $y \equiv y' \pmod{D}$, then from Equation (1.5) again, we have $x \equiv xs + ytD \equiv xs \pmod{D}$. Thus $s \equiv 1 \pmod{D}$ because $\gcd(x, D) = 1$. Since $y = y's + x't \equiv y + xt \pmod{D}$, we have $xt \equiv 0 \pmod{D}$ and so $t \equiv 0 \pmod{D}$. Therefore, the solutions of Equation (1.2) satisfying Equation (1.3) are precisely

$$(x_i + y_i \sqrt{D})(x_0 + y_0 \sqrt{D})^{ng(D)}, n \in \mathbb{Z}. \quad \square$$

We begin by obtaining a formula for $g(D)$. We later discuss the Ankeny-Artin-Chowla and Mordell conjectures, which consider $y_0$ modulo $D$ when $D$ is prime. Afterwards, we establish some technical lemmas which allow us to prove Theorems 5 and 6. Theorems 5 and 6 are our main results, which, together with Theorem 4, tell us how the fundamental solutions of $x^2 - Dy^2 = 1$ can be constructed from the fundamental solutions of $x^2 - D^{2\ell+1}y^2 = 1$ and furthermore that

$$g(D^{2\ell+1}) = \begin{cases} 2D^{2\ell+1} & \text{if } \gcd(x_0, D) = 1 \text{ and } D \text{ is odd}, \\ 2D^{2\ell+1} & \text{if } \gcd(x_0, D) = 2 \text{ and } D \text{ is odd}, \\ D^{2\ell+1} & \text{if } D \text{ is even} \end{cases}$$

for sufficiently large $\ell$.

2. Formula for $g(D)$

In this section, we derive a formula for $g(D)$ in terms of the fundamental solution $x_0 + y_0 \sqrt{D}$.
Theorem 1. Suppose $D$ is a positive integer that is not a perfect square and $x_0 + y_0 \sqrt{D}$ is the fundamental solution of $x^2 - Dy^2 = 1$. Then

$$g(D) = \text{lcm} \left( \text{order}(x_0, D), \frac{D}{\gcd(y_0, D)} \right)$$

(2.1)

where order$(x_0, D)$ is the multiplicative order of $x_0$ in $\mathbb{Z}/D\mathbb{Z}$. In particular, order$(x_0, D) = 1$ if $x_0 \equiv 1 \pmod{D}$ and order$(x_0, D) = 2$ if $x_0 \not\equiv 1 \pmod{D}$.

Proof. We first note that

$$(x_0 + y_0 \sqrt{D})^\ell = \sum_{k=0}^\ell \binom{\ell}{k} x_0^{\ell-k} y_0^k D^{k/2}$$

$$= \sum_{0 \leq 2k \leq \ell} \binom{\ell}{2k} x_0^{\ell-2k} y_0^{2k} D^k + \sqrt{D} \sum_{0 \leq 2k+1 \leq \ell} \binom{\ell}{2k+1} x_0^{\ell-2k-1} y_0^{2k+1} D^k$$

$$= \left( \frac{\ell}{2(0)} \right) x_0^\ell + \sqrt{D} \left( \frac{\ell}{2(0) + 1} \right) x_0^{\ell-1} y_0 \pmod{D}$$

$$= x_0^\ell + \ell x_0^{\ell-1} y_0 \sqrt{D}.$$  

So if $(x_0 + y_0 \sqrt{D})^\ell = 1$ in $(\mathbb{Z}/D\mathbb{Z})[\sqrt{D}]$, then $x_0^\ell \equiv 1 \pmod{D}$ and $\ell x_0^{\ell-1} y_0 \equiv 0 \pmod{D}$. This implies that $\ell y_0 \equiv 0 \pmod{D}$ and hence $\frac{D}{\gcd(y_0, D)} | \ell$. So

$$\text{lcm} \left( \text{order}(x_0, D), \frac{D}{\gcd(y_0, D)} \right) | \ell.$$  

Therefore,

$$g(D) = \text{lcm} \left( \text{order}(x_0, D), \frac{D}{\gcd(y_0, D)} \right).$$

This proves Equation (2.1). The theorem now follows immediately from the fact that $x_0^2 \equiv 1 \pmod{D}$.  

The usual way to find the fundamental solution $x_0 + y_0 \sqrt{D}$ of $x^2 - Dy^2 = 1$ is using the continued fraction expansion of $\sqrt{D}$. We state some well-known properties of continued fractions and the fundamental solutions of $\sqrt{D}$ in next lemma.

Lemma 1. Let $D$ be a positive integer that is not a perfect square. Suppose the continued fraction of $\sqrt{D}$ is $[a_0, a_1, \ldots, a_\ell]$. Then we have

(a) $a_0 = \lfloor \sqrt{D} \rfloor$ and $a_\ell = 2a_0$;

(b) $a_1, \ldots, a_{\ell-1}$ is a palindrome, i.e., $a_j = a_{\ell-j}$ for $1 \leq j \leq \ell - 1$;

(c) Pell’s equation $x^2 - Dy^2 = 1$ has its fundamental solution $x_0 + y_0 \sqrt{D}$ satisfying

$$\frac{x_0}{y_0} = \begin{cases} [a_0, a_1, \ldots, a_\ell] & \text{if } \ell \text{ is even}, \\
[a_0, a_1, \ldots, a_{2\ell-1}] & \text{if } \ell \text{ is odd}. \end{cases}$$
(d) The negative Pell equation \( x^2 - Dy^2 = -1 \) has a solution if and only if \( \ell \) is odd; in this case, the fundamental solution \( x_1 + y_1\sqrt{D} \) satisfies
\[
\frac{x_1}{y_1} = [a_0, a_1, \ldots, a_{\ell-1}].
\]

Proof. See Theorem 5.15 of [12].

In view of Theorem 1, to compute \( g(D) \), we need to determine if \( x_0 \equiv 1 \pmod{D} \) and evaluate \( \gcd(y_0, D) \). Mollin and Srinivasan [13, 14] showed that the values of \( x_0 \pmod{D} \) are closely related to the solvability of the following three generalized Pell equations:
\[
\begin{align*}
x^2 - Dy^2 &= -1, \\
x^2 - Dy^2 &= 2, \\
x^2 - Dy^2 &= -2.
\end{align*}
\tag{2.2}
\]

We first mention a classical result of Perron.

**Theorem 2 ([17]).**

(i) If \( D > 2 \) is a positive integer that is not a perfect square, then at most one of the equations in Equation (2.2) is solvable.

(ii) If \( D = p^\ell \) or \( D = 2p^\ell \) for odd prime \( p \) and \( \ell \geq 1 \), then one and only one equation in Equation (2.2) is solvable.

Proof. Part (i) is Satz 21 of §26 in [17] and part (ii) is Satz 23 of §26 in [17].

For \( D = 2 \), all three equations of Equation (2.2) are clearly solvable.

The following result by Mollin and Srinivasan describes the relation between \( x_0 \pmod{D} \) and the solvability of the equations in Equation (2.2).

**Theorem 3 ([13], [14]).** Let \( D > 2 \) be a positive integer that is not a perfect square. Let \( x_0 + y_0\sqrt{D} \) be the fundamental solution of Pell’s equation
\[
x^2 - Dy^2 = 1.
\tag{2.3}
\]

Then, we have the following.

(i) The negative Pell equation \( x^2 - Dy^2 = -1 \) is solvable if and only if \( x_0 \equiv -1 \pmod{2D} \).

(ii) The equation
\[
x^2 - Dy^2 = 2
\tag{2.4}
\]
is solvable if and only if \( x_0 \equiv 1 \pmod{D} \).

(iii) The equation \( x^2 - Dy^2 = -2 \) is solvable if and only if \( x_0 \equiv -1 \pmod{D} \) and \( x_0 \not\equiv -1 \pmod{2D} \).
**Proof.** In view of Lemma 1(d), the negative Pell equation is solvable if and only if \( \ell \) is odd. Theorem 3 follows readily from Theorem 2 (i), Theorem 4.3 of [13] and Theorem 1.1 of [14]. 

Although Theorem 3 gives a necessary and sufficient condition for \( x_0 \equiv 1 \pmod{D} \), there is no simple condition on \( D \) for the solvability of Equation (2.4). The next few results give simple necessary conditions for the solvability of Equation (2.4).

**Lemma 2.** Suppose \( x^2 - Dy^2 = 2 \) is solvable. If \( p \) is an odd prime factor of \( D \), then \( p \equiv \pm 1 \pmod{8} \). Moreover, if \( D \) is odd, then \( D \equiv 7 \pmod{8} \) and if \( D \) is even, then \( D = 2d \) with odd \( d \) and \( D \equiv \pm 2 \pmod{8} \).

**Proof.** If \( p \) is an odd prime divisor of \( D \), then \( x^2 \equiv 2 \pmod{p} \) is solvable. This implies that \( p \equiv \pm 1 \pmod{8} \).

Suppose \( D \) is odd and \( (x, y) \in \mathbb{N}^2 \) is a solution of Equation (2.4), then either \( x \equiv y \equiv 0 \pmod{2} \) or \( x \equiv y \equiv 1 \pmod{2} \). If \( x \equiv y \equiv 0 \pmod{2} \), then \( x^2 \equiv y^2 \equiv 0 \pmod{4} \). By Equation (2.4), this implies that \( 4 \equiv 2 \pmod{4} \). This is impossible. Hence we must have \( x \equiv y \equiv 1 \pmod{2} \). Then \( x^2 \equiv y^2 \equiv 1 \pmod{8} \). Hence \( D \equiv 7 \pmod{8} \).

If \( D \) is even and \( (x, y) \in \mathbb{N}^2 \) is a solution of Equation (2.4), we write \( D = 2d \). From Equation (2.4), we deduce that \( x \) is even. Hence \( x^2 \equiv 0 \pmod{4} \) and \( Dy^2 \equiv 2 \pmod{4} \). This implies that \( D \equiv 2 \pmod{4} \) and hence \( d \) and \( y \) are odd. Since \( x \) is even, we write \( x = 2x' \). Then we have \( 2(x')^2 - dy^2 = 1 \). Since \( y \) is odd, we have that \( y^2 \equiv 1 \pmod{4} \). If \( x' \) is even, then \( d \equiv -1 \pmod{4} \) and so \( D \equiv -2 \pmod{8} \). If \( x' \) is odd, then \( d \equiv 1 \pmod{4} \) and so \( D \equiv 2 \pmod{8} \).

**Corollary 1.** If \( D \equiv 0, 1 \pmod{4} \), then \( x^2 - Dy^2 = 2 \) is insolvable and hence \( x_0 \not\equiv 1 \pmod{D} \) and \( \text{order}(x_0, D) = 2 \).

**Corollary 2.** Let \( p \) be an odd prime and \( \ell \geq 0 \). Suppose \( x_0 + y_0 \sqrt{p^{2\ell+1}} \) is the fundamental solution of \( x^2 - p^{2\ell+1}y^2 = 1 \). Then \( x_0 \equiv 1 \pmod{p^{2\ell+1}} \) if and only if \( p \equiv 7 \pmod{8} \).

**Proof.** We have that \( x_0 \equiv 1 \pmod{p^{2\ell+1}} \) if and only if \( x^2 - p^{2\ell+1}y^2 = 2 \) is solvable by Theorem 3. So, if \( x_0 \equiv 1 \pmod{p^{2\ell+1}} \), then \( p^{2\ell+1} \equiv 7 \pmod{8} \) and \( p \equiv \pm 1 \pmod{8} \) by Lemma 2 with \( D = p^{2\ell+1} \). Hence \( p \equiv 7 \pmod{8} \). Conversely, if \( p \equiv 7 \pmod{8} \), then \(-1 \) and \(-2 \) are quadratic non-residues modulo \( p \). Hence both \( x^2 - p^{2\ell+1}y^2 = -1 \) and \( x^2 - p^{2\ell+1}y^2 = -2 \) are insolvable. By Theorem 2 (ii) , \( x^2 - p^{2\ell+1}y^2 = 2 \) is solvable and hence \( x_0 \equiv 1 \pmod{p^{2\ell+1}} \).

If the continued fraction of \( \sqrt{D} \) is very simple, we can find out the fundamental solutions explicitly and compute \( g(D) \). For example, if \( \sqrt{D} = [m, \overline{2m}] \), then

\[
g(D) = \begin{cases} 
2(1 + m^2) & \text{for even } m, \\
1 + m^2 & \text{for odd } m;
\end{cases}
\]
and if $\sqrt{D} = [mn, n, 2mn]$, $m, n \in \mathbb{N}, m \geq 2$, then

$$g(D) = \text{lcm} \left( 2, \frac{m^2n^2 + m}{\gcd(2n, m^2n^2 + m)} \right).$$

The next theorem evaluates $g(2^{2\ell+1})$.

**Theorem 4.** For $\ell \geq 1$, we have

$$\left(3 + 2\sqrt{2}\right)^{2\ell-1} = x_0 + y_0\sqrt{2^{2\ell+1}}, \quad (2.5)$$

where $x_0 + y_0\sqrt{2^{2\ell+1}}$ is the fundamental solution of $x^2 - 2^{2\ell+1}y^2 = 1$ and $3 + 2\sqrt{2}$ is the fundamental solution of $x^2 - 2y^2 = 1$. Furthermore, we have that $g(2^{2\ell+1}) = 2^{2\ell+1}$.

**Proof.** We prove Equation (2.5) by induction on $\ell \geq 1$. For $\ell = 1$, we have

$$\left(3 + 2\sqrt{2}\right)^{2(1)-1} = 3 + 3\sqrt{2} = 3 + \sqrt{2(1)^2 + 1}$$

so $x_0 = 3$ and $y_0 = 1$. Thus Equation (2.5) is true for $\ell = 1$.

Suppose

$$\left(3 + 2\sqrt{2}\right)^{2\ell-1} = s + t\sqrt{2^{2\ell+1}} = s + t\ell \sqrt{2}$$

for some odd integers $s, t \in \mathbb{N}$. Then

$$\left(3 + 2\sqrt{2}\right)^{2\ell} = (s + t\ell \sqrt{2})^2 = (s^2 + 2^{2\ell+1}t^2) + st\sqrt{2^{2(\ell+1)}+1}.$$ 

so $x_0 = s^2 + 2^{2\ell+1}t^2$ and $y_0 = st$. Clearly, $x_0$ and $y_0$ are odd because $s$ and $t$ are odd. This proves Equation (2.5).

Clearly $(x_0, y_0)$ in Equation (2.5) is a solution of $x^2 - 2^{2\ell+1}y^2 = 1$. If $(x_1, y_1) \in \mathbb{N}^2$ is the fundamental solution of $x^2 - 2^{2\ell+1}y^2 = 1$, then

$$x_0 + y_0\sqrt{2^{2\ell+1}} = (x_1 + y_1\sqrt{2^{2\ell+1}})^j$$

for some $j \in \mathbb{N}$. On the other hand, $(x_1, y_12^\ell)$ is also a solution of $x^2 - 2y^2 = 1$. Hence

$$x_1 + y_12^\ell \sqrt{2} = (3 + 2\sqrt{2})^i$$

for some $i \in \mathbb{N}$. Therefore, from Equation (2.5), we have

$$\left(3 + 2\sqrt{2}\right)^{2i-1} = x_0 + y_0\sqrt{2^{2i+1}} = (x_1 + y_1\sqrt{2^{2i+1}})^j = (3 + 2\sqrt{2})^{ij}.$$ 

So $ij = 2\ell-1$ and $i = 2^m$ for some $m \geq 0$. In view of Equation (2.5), we have

$$x_1 + y_1\sqrt{2^{2\ell+1}} = (3 + 2\sqrt{2})^i = (3 + 2\sqrt{2})^{2^m} = x_0 + y_0\sqrt{2^{2(2^m+1)+1}}$$

as desired.
with odd $x'_0, y'_0 \in \mathbb{N}$. Since both $y_1$ and $y'_0$ are odd, we have that $\ell = m + 1$. Therefore, $j = 1$ and we conclude that $x_0 + y_0\sqrt{2^{2\ell+1}} = x_1 + y_1\sqrt{2^{2\ell+1}}$ is the fundamental solution of $x^2 - 2^{2\ell+1}y^2 = 1$.

In view of Lemma 2, the equation $x^2 - 2^{2\ell+1}y^2 = 2$ is insolvable for $\ell \geq 1$. Hence $x_0 \not\equiv 1 \pmod{2^{2\ell+1}}$ and order $(x_0, 2^{2\ell+1}) = 1$. Therefore, we have

$$g(2^{2\ell+1}) = \text{lcm}\left(1, \frac{2^{2\ell+1}}{\gcd(y_0, 2^{2\ell+1})}\right) = 2^{2\ell+1}$$

for $\ell \geq 1$. This completes the proof. \hfill \Box

3. Ankeny, Artin and Chowla’s Conjecture and Mordell’s Conjecture

In this section, we study $g(p)$ for odd primes $p$. In view of Theorem 1, it is important to determine if $p | y_0$, where $x_0 + y_0\sqrt{p}$ is the fundamental solution of $x^2 - py^2 = 1$.

Based on numerical checking for the first 1000 primes $p$, we find that $p$ does not divide $y_0$. We are led to conjecture the following.

**Conjecture 1.** Let $p$ be an odd prime and $x_0 + y_0\sqrt{p}$ be the fundamental solution of $x^2 - py^2 = 1$. Then $p \nmid y_0$. Hence

$$g(p) = \begin{cases} p & \text{if } p \equiv 7 \pmod{8}, \\
2p & \text{if } p \not\equiv 7 \pmod{8}. \end{cases}$$

There is a famous conjecture of Ankeny, Artin and Chowla (AAC conjecture) (Conjecture 2 below) in [3] concerning the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{p})$ where $p$ is a prime congruent to 1 modulo 4. Mordell also made a conjecture (Conjecture 3 below) in [16] similar in nature to the AAC conjecture for a prime $p$ congruent to 3 modulo 4. Both conjectures are still unsolved but are widely believed to be true. The AAC conjecture was first verified for all primes not exceeding $10^{11}$ by Van Der Poorten et al. in [18] and then for all primes not exceeding $2(10^{11})$ in [19]. In [15], Mordell proved the AAC conjecture for any regular prime $p$, i.e., when $p$ does not divide the class number of the number field $\mathbb{Q}\left(e^{\frac{2\pi i}{p}}\right)$.

The conjecture of Mordell has also been verified for all primes not exceeding $10^7$ in [5]. Both the AAC conjecture and Mordell’s conjecture are widely studied. For more discussion on these conjectures, we refer readers to [1], [7], and [9].

**Conjecture 2 ([3]).** Let $p$ be a prime congruent to 1 modulo 4 and $\frac{1}{2}(a + b\sqrt{p})$ be the fundamental unit for $\mathbb{Q}(\sqrt{p})$ where $a, b \in \mathbb{N}$ and $a \equiv b \pmod{2}$. Then $p \nmid b$.

**Conjecture 3 ([16]).** Let $p$ be a prime congruent to 3 modulo 4. Let $x_0 + y_0\sqrt{p}$ be the fundamental solution of $x^2 - py^2 = 1$. Then $p \nmid y_0$. 
Conjecture 1 is exactly the same as Mordell’s conjecture for \( p \equiv 3 \pmod{4} \). By using the relation between the fundamental unit for \( \mathbb{Q}(\sqrt{p}) \) and the fundamental solutions of \( x^2 - py^2 = 1 \), it can be shown that Conjecture 1 is the same as the AAC Conjecture for \( p \equiv 1 \pmod{4} \).

**Corollary 3.** If Ankeny, Artin and Chowla’s conjecture and Mordell’s conjecture are true, then for any odd prime \( p \) and \( \ell \geq 0 \), we have

\[
g(p^{2\ell+1}) = \begin{cases} 
p^{2\ell+1} & \text{if } p \equiv 7 \pmod{8}, \\
2p^{2\ell+1} & \text{if } p \not\equiv 7 \pmod{8}.
\end{cases}
\]

**Proof.** This follows readily from Corollary 4 and \( \gcd(y_0, p^{2\ell+1}) = 1 \). \( \Box \)

From our gathered data, we observe that for \( D = 2p \) we have \( \gcd(y_0, 2p) = 2 \) for all odd primes \( p \) except for \( p = 23 \). We present an analogue of the AAC and Mordell’s conjecture in which \( p \) is replaced by \( 2p \).

**Conjecture 4.** Let \( p \) be an odd prime and \( x_0 + y_0\sqrt{2p} \) be the fundamental solution of \( x^2 - 2py^2 = 1 \). Then \( \gcd(y_0, 2p) = 2 \) except when \( p = 23 \). For \( p = 23 \), \( \gcd(y_0, 2(23)) = 46 \). Hence for \( p \neq 23 \)

\[
g(2p) = \begin{cases} 
p & \text{if order } (x_0, 2p) = 1, \\
2p & \text{if order } (x_0, 2p) = 2.
\end{cases}
\]

### 4. The Order \( g(D^{2\ell+1}) \)

In this section, we study the order \( g(D^{2\ell+1}) \). In view of Theorem 1, we need to find the relation between the fundamental solutions \( x_0 + y_0\sqrt{D} \) and \( x_1 + y_1\sqrt{D^{2\ell+1}} \) of \( x^2 - Dy^2 = 1 \) and \( x^2 - D^{2\ell+1}y^2 = 1 \), respectively. Since

\[
1 = x_1^2 - D^{2\ell+1}y_1^2 = x_1^2 - D(D^\ell y_1)^2,
\]

we have that \( x_1 + y_1\sqrt{D^{2\ell+1}} \) is a power of \( x_0 + \sqrt{D}y_0 \). Theorem 5 below gives us the exact power of \( x_0 + \sqrt{D}y_0 \). The prime number 3 is special among all other prime numbers in this aspect. Although the values of \( g(p) \) are still undetermined (c.f. Ankeny, Artin and Chowla’s and Mordell’s conjectures), Theorem 6 below gives the values of \( g(D^{2\ell+1}) \) for sufficiently large \( \ell \).

For any prime number \( p \) and \( m \in \mathbb{N} \), we define the exact power of \( p \) dividing \( m \) by \( n_p(m) \), that is, \( p^{n_p(m)} \parallel m \). Here \( d^n \parallel m \) if \( d^n \mid m \) but \( d^{n+1} \nmid m \).

**Lemma 3.** Let \( D \) be a positive integer that is not a perfect square. Suppose \( (x_0, y_0) \) is a solution of \( x^2 - Dy^2 = 1 \) such that \( 3 \nmid y_0 \) and

\[
(x_0 + y_0\sqrt{D})^3 = x_0' + y_0'\sqrt{D}
\]
with \( \ell_1 := n_3(y_0') \geq 1 \) and \( y_0' = 3^{\ell_1}y_0z_0 \) for some \( z_0 \in \mathbb{N} \) with \( 3 \nmid z_0 \) and \( \gcd(z_0, D) = 1 \). Then for any \( \ell \geq 1 \), we have

\[
(x_0 + y_0\sqrt{D})^{3^\ell} = x_1 + y_1\sqrt{D}
\]

with \( n_3(y_1) = \ell + \ell_1 - 1 \) and \( y_1 = 3^{\ell+\ell_1-1}y_0z_1 \) for some \( z_1 \in \mathbb{N} \) with \( 3 \nmid z_1 \) and \( \gcd(z_1, D) = 1 \).

**Proof.** We prove the lemma by induction on \( \ell \geq 1 \). The case \( \ell = 1 \) is true by assumption. Suppose

\[
(x_0 + y_0\sqrt{D})^{3^\ell} = x_1 + y_1\sqrt{D}
\]

with \( n_3(y_1) = \ell + \ell_1 - 1 \) and \( y_1 = 3^{\ell+\ell_1-1}y_0z_1 \) for some \( z_1 \in \mathbb{N} \) with \( 3 \nmid z_1 \) and \( \gcd(z_1, D) = 1 \). We see that

\[
(x_0 + y_0\sqrt{D})^{3^{\ell+1}} = (x_1 + y_1\sqrt{D})^3 = (x_1^3 + 3x_1y_1^2D) + (3x_1^2y_1 + y_1^3D)\sqrt{D}.
\]

Since \( x_1^2 - Dy_1^2 = 1 \) and \( 3 \mid y_1 \), we must have that \( 3 \nmid x_1 \). We conclude that

\[
n_3(x_1^3 + 3x_1y_1^2D) = 0
\]

and

\[
n_3(3x_1^2y_1 + y_1^3D) = n_3 \left( 3y_1 \left( x_1^2 + \frac{y_1^2D}{3} \right) \right) = n_3(3y_1) = \ell + \ell_1.
\]

Moreover,

\[
3x_1^2y_1 + y_1^3D = y_1 \left( 3x_1^2 + y_1^2D \right) = 3^{\ell+\ell_1}y_0z_1 \left( x_1^2 + 3^{2\ell+2\ell_1-3}y_0^2z_1^2D \right) = 3^{\ell+\ell_1}y_0z_1'
\]

for some \( z_1' \in \mathbb{N} \) and \( 3 \nmid z_1' \) and \( \gcd(z_1', D) = 1 \) because \( \gcd(x_1, D) = 1 \). This proves the lemma.

**Lemma 4.** Let \( D \in \mathbb{N} \) and let \( M \in \mathbb{N} \) be such that \( p \mid D \) if \( p \mid M \). Then we have

\[
DM \mid \left( \frac{M}{2j+1} \right) D^j
\]

for any \( 2 \leq j \leq (M-1)/2 \).

**Proof.** We first note that we can write

\[
\left( \frac{M}{2j+1} \right) D^j = (DM) \left( \frac{(M-1)\cdots(M-2j)D^{j-1}}{(2j+1)!} \right).
\]  \hfill (4.1)

It suffices to show that

\[
n_p(DM) \leq n_p \left( \frac{M}{2j+1} \right) D^j
\]  \hfill (4.2)
for all primes $p \mid D$. It is well-known that for any prime $p$ and $m \in \mathbb{N}$, we have

$$n_p(m!) = \left\lfloor \frac{m}{p} \right\rfloor + \left\lfloor \frac{m}{p^2} \right\rfloor + \cdots \leq \frac{m}{p} + \frac{m}{p^2} + \cdots$$

$$= m \sum_{n=1}^{\infty} \frac{1}{p^n} = m \left( 1 - \frac{1}{p} \right) = \frac{m}{p-1}$$

(4.3)

where $\lfloor \xi \rfloor$ is the greatest integer $\leq \xi$.

Let $p$ be a prime dividing $D$. Consider first the case that $p \geq 5$. In view of Equation (4.3), we have $n_p((2j + 1)!) \leq \frac{2j+1}{p-1} \leq \frac{2j+1}{4}$ and hence $n_p((2j + 1)!) \leq \left\lfloor \frac{2j+1}{4} \right\rfloor$. This implies that for all $2 \leq j \leq (M-1)/2$ and $p \geq 5$, we have

$$n_p((2j + 1)!) \leq \frac{2j+1}{4} \leq \frac{j}{2} \leq j - 1 \leq n_p(D)(j - 1) = n_p(D^{j-1}).$$

In view of Equation (4.1), this shows Equation (4.2) for $p_k \geq 5$.

Now, suppose $p = 2$. Note that $5! = 2^3(15)$ and $7! = 2^4(315)$, so $n_2(5!) = 3$ and $n_2(7!) = 4$. Since $2^3 \mid (M - 1)(M - 2)(M - 3)(M - 4)$ and $2^4 \mid (M - 1)(M - 2)(M - 3)(M - 4)(M - 5)(M - 6)$, we use Equation (4.1) to conclude that

$$n_2(DM) \leq n_2 \left( \left( \frac{M}{2j+1} \right) D^j \right)$$

for $j = 2, 3$. For $j \geq 4$, among $M - 1, M - 2, \ldots, M - 2j$, there are $j$ even numbers and at least two of them are divisible by 4 because there are more than 8 consecutive integers. Thus, $2^{j+2} \mid (M - 1) \cdots (M - 2j)$. Note also that, by Equation (4.3), $n_2((2j + 1)!) \leq \frac{2j+1}{2j+1} = 2j + 1$. It then follows that

$$n_2 \left( (M - 1) \cdots (M - 2j) D^{j-1} \right) \geq n_2(D)(j - 1) + (j + 2) \geq j - 1 + j + 2 = 2j + 1 \geq n_2((2j + 1)!)$$

and hence $n_2(DM) \leq n_2 \left( \left( \frac{M}{2j+1} \right) D^j \right)$ for $j \geq 4$. This proves Equation (4.2) for $p = 2$.

Finally, suppose $p = 3$. Then, by Equation (4.3), $n_3((2j + 1)!) \leq \frac{2j+1}{3-1} = \frac{2j+1}{2} \leq j + \frac{1}{2}$ and so $n_3((2j + 1)!) \leq j$. For $j \geq 2$, among $M - 1, M - 2, \ldots, M - 2j$, there are more than 4 consecutive integers. Thus, $3 \mid (M - 1) \cdots (M - 2j)$. It then follows that

$$n_3 \left( (M - 1) \cdots (M - 2j) D^{j-1} \right) \geq n_3(D)(j - 1) + 1 \geq (j - 1) + 1 = j \geq n_3((2j + 1)!)$$

and hence $n_3(DM) \leq n_3 \left( \left( \frac{M}{2j+1} \right) D^j \right)$. This proves Equation (4.2) for $p = 3$.

Therefore, we have proved Equation (4.2) for all $p \mid D$ and thus we have proved the lemma. □
Lemma 5. Let $D$ be a positive integer that is not a perfect square and $M \in \mathbb{N}$ be such that $p \mid D$ if $p \mid M$. If $(x_0, y_0) \in \mathbb{N}^2$ is a solution of $x^2 - Dy^2 = 1$ and

$$(x_0 + y_0\sqrt{D})^M = x_1 + y_1\sqrt{D}$$

for some $x_1, y_1 \in \mathbb{N}$, then $\gcd(x_1, D) = 1$ and $y_1 = My_0y_2$ with

$$\gcd(y_2, D) = \begin{cases} 3 & \text{if } 3 \nmid y_0, 3 \nmid D, \frac{D}{3} \equiv -1 \pmod{3}, \text{ and } 3 \mid M, \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Suppose $M \in \mathbb{N}$ such that $p \mid D$ if $p \mid M$. Then we have

$$(x_0 + y_0\sqrt{D})^M = \sum_{j=0}^{M} \binom{M}{j} x_0^{M-j}(y_0\sqrt{D})^j$$

$$= \sum_{0 \leq j \leq M/2} \binom{M}{2j} x_0^{M-2j} y_0^{2j} D^j + \sum_{0 \leq j \leq (M-1)/2} \binom{M}{2j+1} x_0^{M-2j-1}(y_0\sqrt{D})^{2j+1}$$

$$= \sum_{0 \leq j \leq M/2} \binom{M}{2j} x_0^{M-2j} y_0^{2j} D^j + \sqrt{D} \sum_{0 \leq j \leq (M-1)/2} \binom{M}{2j+1} x_0^{M-2j-1}(y_0\sqrt{D})^{2j+1}$$

$$:= x_1 + y_1\sqrt{D}.$$ 

It is known that $(x_1, y_1)$ is also a solution of $x^2 - Dy^2 = 1$. Thus, $\gcd(x_1, D) = 1$. We now consider $y_1$. In view of Lemma 4, we can write

$$\sum_{2 \leq j \leq (M-1)/2} \binom{M}{2j+1} x_0^{M-2j-1} y_0^{2j+1} D^j = DMy_0z$$

for some $z \in \mathbb{N}$. Hence we have

$$y_1 = \sum_{0 \leq j \leq (M-1)/2} \binom{M}{2j+1} x_0^{M-2j-1} y_0^{2j+1} D^j$$

$$= Mx_0^{M-1} y_0 + \binom{M}{3} x_0^{M-3} y_0^3 D + DMy_0z$$

$$= My_0 \left( x_0^{M-1} + \frac{(M-1)(M-2)}{6} y_0^2 Dx_0^{M-3} + Dz \right) = My_0y_2$$

where

$$y_2 := x_0^{M-1} + \frac{(M-1)(M-2)}{6} y_0^2 Dx_0^{M-3} + Dz.$$ 

It remains to evaluate

$$\gcd(y_2, D) = \gcd \left( x_0^{M-1} + \frac{(M-1)(M-2)}{6} y_0^2 Dx_0^{M-3}, D \right).$$ \hspace{1cm} (4.4)$$
If $3
mid D$, then $3
mid M$ and $6 \mid (M-1)(M-2)$. Hence from Equation (4.4), we have $\gcd(y_2, D) = \gcd(x_0^{M-1}, D) = 1$.

We now suppose $3 \nmid D$.

If $3 \nmid y_0$, then $6 \mid (M-1)(M-2)y_0^2$. Hence from Equation (4.4), we have $\gcd(y_2, D) = \gcd(x_0^{M-1}, D) = 1$.

If $3 \nmid y_0$, then

$$\gcd(y_2, D) = \gcd\left(x_0^{M-1} + \frac{(M-1)(M-2)}{2} y_0^2 \left(\frac{D}{3}\right), x_0^{M-3}, D\right) = \gcd\left(1 + \frac{(M-1)(M-2)}{2} y_0^2 \left(\frac{D}{3}\right), D\right)$$

because $\gcd(x_0, D) = 1$ and $x_0^2 - Dy_0^2 = 1$. Let $p$ be a prime such that $p \mid D$ and $p \neq 3$. Then, $p \mid \frac{D}{3}$ and so

$$p \nmid 1 + \frac{(M-1)(M-2)}{2} y_0^2 \left(\frac{D}{3}\right).$$

Hence the only possible prime divisor of $\gcd\left(1 + \frac{(M-1)(M-2)}{2} y_0^2 \left(\frac{D}{3}\right), D\right)$ is 3.

If $3^2 \mid D$, then $3 \mid \frac{D}{3}$ and hence $3 \nmid 1 + \frac{(M-1)(M-2)}{2} y_0^2 \left(\frac{D}{3}\right)$. It follows that $\gcd(y_2, D) = \gcd\left(1 + \frac{(M-1)(M-2)}{2} y_0^2 \left(\frac{D}{3}\right), D\right) = 1$.

If $3\|D$, then $\gcd\left(1 + \frac{(M-1)(M-2)}{2} y_0^2 \left(\frac{D}{3}\right), D\right) = 1$ or 3. Also we have

$$\gcd\left(1 + \frac{(M-1)(M-2)}{2} y_0^2 \left(\frac{D}{3}\right), D\right) = 3$$

if and only if

$$1 + \frac{(M-1)(M-2)}{2} y_0^2 \left(\frac{D}{3}\right) \equiv 0 \pmod{3}$$

if and only if

$$\frac{(M-1)(M-2)}{2} \left(\frac{D}{3}\right) \equiv 2 \pmod{3}$$

because $3 \nmid y_0$ and hence $y_0^2 \equiv 1 \pmod{3}$. Since $3 \mid \frac{D}{3}$, we have that $\frac{D}{3} \equiv \pm 1 \pmod{3}$.

If $\frac{D}{3} \equiv 1 \pmod{3}$, then

$$\frac{(M-1)(M-2)}{2} \left(\frac{D}{3}\right) \equiv 2 \pmod{3}$$

if and only if $(M-1)(M-2) \equiv 1 \pmod{3}$. However, $(M-1)(M-2) \neq 1 \pmod{3}$ for any $M \in \mathbb{Z}$. So if $\frac{D}{3} \equiv 1 \pmod{3}$, then $\gcd(y_2, D) = 1$ by Equation (4.3).
If $\frac{D}{3} \equiv -1 \pmod{3}$, then $\gcd\left(1 + \frac{(M-1)(M-2)}{2}y_0^2 \left(\frac{D}{3}\right), D\right) = 3$ if and only if $\frac{(M-1)(M-2)}{2} \equiv 1 \pmod{3}$ if and only if $3 \mid M$. We conclude that

$$\gcd(y_2, D) = \begin{cases} 3 & \text{if } 3 \nmid y_0, 3 \mid D, \frac{D}{3} \equiv -1 \pmod{3}, \text{and } 3 \mid M, \\ 1 & \text{otherwise.} \end{cases}$$

\[\square\]

**Theorem 5.** Let $D$ be a positive integer that is not a perfect square and let $x_0 + y_0 \sqrt{D}$ be the fundamental solution of $x^2 - Dy^2 = 1$. Suppose $D^{\ell_0} \mid y_0$ for some $\ell_0 \geq 0$ and $\ell_1 := n_3 \left(3x_0^2 y_0 + Dy_0^3\right)$. We have three cases:

(i) In the case that $0 \leq \ell \leq \ell_0$, we have that $(x_0, y_0 D^{-\ell})$ is the fundamental solution of $x^2 - D^{2\ell+1}y = 1$.

(ii) In the case that $\ell_0 < \ell$ and

$$3 \nmid y_0, 3 \mid D, \text{ and } \frac{D}{3} \equiv -1 \pmod{3} \quad (4.5)$$

we have that if

$$(x_0 + y_0 \sqrt{D})^{3 \min\{\ell, \ell_1\} - 1 \gcd(D^\ell, y_0)} = x_1 + y_1 \sqrt{D}$$

then $n_3(y_1) = \max\{\ell, \ell_1\}$, $D^\ell \mid y_1$, and $(x_1, y_1 D^{-\ell})$ is the fundamental solution of $x^2 - D^{2\ell+1}y^2 = 1$.

(iii) In the case that $\ell_0 < \ell$ and Equation (4.5) does not hold, we have that if

$$(x_0 + y_0 \sqrt{D})^{\frac{D^\ell}{\gcd(D^\ell, y_0)}} = x_1 + y_1 \sqrt{D}$$

then $D^\ell \mid y_1$ and $(x_1, y_1 D^{-\ell})$ is the fundamental solution of $x^2 - D^{2\ell+1}y^2 = 1$.

**Proof.** Suppose $x_0 + y_0 \sqrt{D}$ is the fundamental solution of $x^2 - Dy^2 = 1$ and $D^{\ell_0} \mid y_0$. We write $y_0 = D^{\ell_0} ab$ for some $a, b \in \mathbb{N}$ with $\gcd(b, D) = 1$ and $p \mid D$ for any $p \mid a$.

(i) For $0 \leq \ell \leq \ell_0$, since

$$1 = x_0^2 - Dy_0^2 = x_0^2 - D^{2\ell+1}(D^{\ell_0-\ell} ab)^2$$

so $(x_0, D^{\ell_0-\ell} ab) = (x_0, y_0 D^{-\ell}) \in \mathbb{N}^2$ is a solution of $x^2 - D^{2\ell+1}y^2 = 1$. We claim that $(x_0, y_0 D^{-\ell})$ is the smallest such solution. Indeed, if $(s, t) \in \mathbb{N}^2$ is any solution of $x^2 - D^{2\ell+1}y^2 = 1$, then $(s, D^\ell t)$ is a solution of $x^2 - Dy^2 = 1$ and hence $s \geq x_0$.
We will show that $N$ so that with $z$

Note that ($N$ for some $M$ with $\ell > \ell$. Thus, $(x_0, y_0 D^{-t})$ is the minimal solution and hence the fundamental solution of $x^2 - D^{2\ell+1} y^2 = 1$. This proves part (i).

(ii) Now, we consider the case in which $\ell > \ell_0$ and Equation (4.5) holds. We write

$$ (x_0 + y_0 \sqrt{D})^\frac{D^\ell}{\gcd(D^\ell, y_0)} = x_1 + y_1 \sqrt{D}. $$

Note that $(x_1, y_1)$ is a solution of $x^2 - Dy^2 = 1$. By Lemma 3, we can write

$$ (x_0 + y_0 \sqrt{D})^{\ell - \min\{\ell, \ell_1\} + 1} = x_0' + y_0' \sqrt{D} $$

with $n_3(y_0) = \ell - \min\{\ell, \ell_1\} + \ell_1 = \max\{\ell, \ell_1\}$ and $y_0' = 3^{\max\{\ell, \ell_1\}} y_0 z_0$ for some $z_0 \in \mathbb{N}$ with $3 \nmid z_0$. It follows from this and Lemma 5 that

$$ (x_0 + y_0 \sqrt{D})^{\frac{D^\ell}{\gcd(D^\ell, y_0)}} = (x_0' + y_0' \sqrt{D})^{\frac{(D/3)^\ell}{\gcd(D^\ell, y_0)}} = x_1 + y_1 \sqrt{D} \quad (4.6) $$

with

$$ y_1 = \frac{(D/3)^\ell}{\gcd(D^\ell, y_0)} y_0' y_2 = \left(\frac{D}{3}\right)^\ell 3^{\max\{\ell, \ell_1\}} \left(\frac{y_0}{\gcd(D^\ell, y_0)}\right) z_0 y_2 $$

so that $D^\ell | y_1$ and $n_3(y_1) = n_3(y_0') = \max\{\ell, \ell_1\}$. So, we have that $(x_1, y_1 D^{-t})$ is a solution of $x^2 - D^{2\ell+1} y^2 = 1$. We claim that $(x_1, y_1 D^{-t})$ is the fundamental solution of $x^2 - D^{2\ell+1} y^2 = 1$. Suppose $(s, t)$ is the fundamental solution of $x^2 - D^{2\ell+1} y^2 = 1$. Then,

$$ x_1 + y_1 \sqrt{D} = \left(s + t D^\ell \sqrt{D}\right)^N $$

for some $N \in \mathbb{N}$. On the other hand, $(s, t D^\ell) \in \mathbb{N}^2$ is a solution of $x^2 - Dy^2 = 1$, so

$$ s + t D^\ell \sqrt{D} = (x_0 + y_0 \sqrt{D})^M \quad (4.7) $$

for some $M \in \mathbb{N}$. Therefore, we have

$$ (x_0 + y_0 \sqrt{D})^{\frac{D^\ell}{\gcd(D^\ell, y_0)}} = x_1 + y_1 \sqrt{D} = \left(s + t D^\ell \sqrt{D}\right)^N = (x_0 + y_0 \sqrt{D})^{NM}. $$

We will show that $N = 1$. Note that

$$ M | \frac{D^\ell}{3^{\min\{\ell, \ell_1\} - 1} \gcd(D^\ell, y_0)}. \quad (4.8) $$
Using Equation (4.7) and Lemma 5, we have that \( M y_0 y_2 = t D^\ell \). Again using Lemma 5, if \( 3 \mid M \), then \( 3 \mid y_0 y_2 \) which contradicts \( 3 \mid t D^\ell \). So, we have that \( 3 \nmid M \).

Let \( M_1 \) be such that \( M = 3^{n_3(M)} M_1 \) and \( 3 \nmid M_1 \). By Lemmas 3 and 5, we have
\[
s + t D^\ell \sqrt{D} = (x_0 + y_0 \sqrt{D})^{3^{n_3(M)} M_1} = (a + b \sqrt{D})^{M_1},
\]
with \( t D^\ell = M_1 a y_2' \), where \( n_3(a) = n_3(M) + \ell_1 - 1 \) and \( 3 \nmid y_2' \). Hence
\[
n_3(M_1 a y_2') = n_3(a) = n_3(M) + \ell_1 - 1 \geq n_3(D) \ell = \ell
\]
and furthermore
\[
n_3\left( \frac{D^\ell}{3^{\min\{\ell, \ell_1\}} \gcd(D^\ell, y_0)} \right) = \ell - \min\{\ell, \ell_1\} + 1 \leq n_3(M)
\]
by Equation (4.9).

For primes \( p \mid D \) with \( p \neq 3 \), we use \( M y_0 y_2 = t D^\ell \) with \( \gcd(y_2, D) = 3 \) from Equation (4.7) to get
\[
n_p(M) + n_p(y_0) \geq n_p(D) \ell,
\]
and furthermore
\[
n_p\left( \frac{D^\ell}{3^{\min\{\ell, \ell_1\}} \gcd(D^\ell, y_0)} \right) = n_p\left( \frac{D^\ell}{\gcd(D^\ell, y_0)} \right) = n_p(D) \ell - \min\{n_p(D) \ell, n_p(y_0)\}
\leq n_p(M)
\]
by Equation (4.10). Therefore, we have shown that any prime power that divides \( \frac{D^\ell}{3^{\min\{\ell, \ell_1\}} \gcd(D^\ell, y_0)} \) divides \( M \). Together with Equation (4.8), we conclude that
\[
M = \frac{D^\ell}{3^{\min\{\ell, \ell_1\}} \gcd(D^\ell, y_0)}
\]
and hence \( N = 1 \). Thus \( (x_1, y_1 D^{-\ell}) \) is the fundamental solution of \( x^2 - D^{2\ell+1} y^2 = 1 \).

(iii) Now, we consider the case in which \( \ell > \ell_0 \) and Equation (4.5) does not hold. We write
\[
(x_0 + y_0 \sqrt{D})^{\frac{D^\ell}{\gcd(D^\ell, y_0)}} = x_1 + y_1 \sqrt{D}.
\]
Note that \( (x_1, y_1) \) is a solution of \( x^2 - D y^2 = 1 \) and, by Lemma 5, \( D^\ell \mid y_1 \). So, we have that \( (x_1, y_1 D^{-\ell}) \) is a solution of \( x^2 - D^{2\ell+1} y^2 = 1 \). We claim that \( (x_1, y_1 D^{-\ell}) \) is the fundamental solution of \( x^2 - D^{2\ell+1} y^2 = 1 \). Suppose \( (s, t) \) is the fundamental solution of \( x^2 - D^{2\ell+1} y^2 = 1 \). Then, as in case (ii), we have
\[
(x_0 + y_0 \sqrt{D})^{\frac{D^\ell}{\gcd(D^\ell, y_0)}} = x_1 + y_1 \sqrt{D} = \left( s + t D^\ell \sqrt{D} \right)^N = (x_0 + y_0 \sqrt{D})^{N M}
\]
for some \( N, M \in \mathbb{N} \). Hence \( \frac{D^t}{\gcd(D^t,y_0)} = NM \) and so \( M \mid \frac{D^t}{\gcd(D^t,y_0)} \). Using Lemma 5, we may write \( M y_0 y_2 = t D^t \) where \( y_2 \in \mathbb{N} \) with \( \gcd(y_2, D) = 1 \). So, \( M = \left( \frac{t}{y_0 y_2} \right) D^t \).

Since \( \gcd(y_2, D) = 1 \), we must have that \( \frac{\gcd(D^t,y_0)}{\gcd(D^t,y_0)} \mid M \). We conclude that \( M = \frac{D^t}{\gcd(D^t,y_0)} \), so \( N = 1 \) and \( (x_1, y_1 D^{-\ell}) \) is the fundamental solution of \( x^2 - D^{2\ell+1} y^2 = 1 \). Additionally, we use Lemma 5 to get that \( y_1 = \frac{D^t}{\gcd(D^t,y_0)} y_0 y_2 D^t \frac{y_0}{\gcd(D^t,y_0)} y_2 \) with \( \gcd(y_2, D) = 1 \), so \( D \mid \frac{y_0}{\gcd(D^t,y_0)} y_2 \) and thus \( D^t \mid y_1 \). This proves part (iii). □

In view of Theorem 5, we are now able to evaluate \( g(D^{2\ell+1}) \) for sufficiently large \( \ell \).

**Theorem 6.** Let \( D > 2 \) be a positive integer which is not a perfect square and \( x_0 + y_0 \sqrt{D} \) is the fundamental solution of \( x^2 - D^2 y^2 = 1 \). If Equation (4.5) does not hold and \( \ell \geq \max\{\ell_0 + 1, \lfloor n_p(y_0)/n_p(D) \rfloor : p \mid D\} \), or Equation (4.5) holds and \( \ell \geq \max\{\ell_0 + 1, \ell_1, \lfloor n_p(y_0)/n_p(D) \rfloor : p \mid D, p \neq 3\} \) where \( \ell_0 \) and \( \ell_1 \) are defined as in Theorem 5, then we have

\[
g(D^{2\ell+1}) = \begin{cases} 
D^{2\ell+1} & \text{if order}(x_0, D) = 1 \text{ and } D \text{ is odd}, \\
2D^{2\ell+1} & \text{if order}(x_0, D) = 2 \text{ and } D \text{ is odd}, \\
D^{2\ell+1} & \text{if } D \text{ is even}.
\end{cases}
\]

**Proof.** Suppose Equation (4.5) does not hold and \( \ell > \ell_0 \). By Theorem 5,

\[
\left(x_0 + y_0 \sqrt{D}\right)^{\frac{D^t}{\gcd(D^t,y_0)}}
\]

is the fundamental solution of \( x^2 - D^{2\ell+1} y^2 = 1 \). In view of Lemma 5, we have

\[
\left(x_0 + y_0 \sqrt{D}\right)^{\frac{D^t}{\gcd(D^t,y_0)}} = x_1 + \frac{D^t}{\gcd(D^t,y_0)} y_0 y_2 \sqrt{D} = x_1 + y_1 \sqrt{D^{2\ell+1}},
\]

with \( y_1 = \frac{y_0 y_2}{\gcd(D^t,y_0)} \) and \( \gcd(y_2, D) = 1 \). In view of Theorem 1, we need to evaluate \( \text{order}(x_1, D^{2\ell+1}) \) and \( \frac{D^{2\ell+1}}{\gcd(D^{2\ell+1},y_1)} \). So if \( \ell \geq \frac{n_p(y_0)}{n_p(D)} \) for all \( p \mid D \), then \( \gcd(D^t,y_0) = y_0 \) and \( y_1 = y_2 \). Hence \( \gcd(y_1, D) = 1 \). So \( \frac{D^{2\ell+1}}{\gcd(D^{2\ell+1},y_1)} = D^{2\ell+1} \).

Suppose Equation (4.5) holds and \( \ell > \ell_0 \). By Theorem 5,

\[
\left(x_0 + y_0 \sqrt{D}\right)^{\frac{D^t}{\gcd(D^t,y_0)}}
\]

is the fundamental solution of \( x^2 - D^{2\ell+1} y^2 = 1 \). In the proof of (ii) of Theorem 5 and Equation (4.6), we have

\[
(x_0 + y_0 \sqrt{D})^{\frac{D^t}{\gcd(D^t,y_0)}} = x_1 + y_1 \sqrt{D^{2\ell+1}}
\]
with
\[ y_1 = 3^{\max\{\ell, \ell_1\} - \ell} \left( \frac{y_0}{\gcd(D^\ell, y_0)} \right) \]  
and \( \gcd(D, z_0 y_2) = 1 \). So, if \( \ell \geq \max\{\ell_1, n_p(y_0) / n_p(D) : p \mid D, p \neq 3\} \), then
\[ \max\{\ell, \ell_1\} - \ell = 0 \]  
and \( \gcd(D^\ell, y_0) = y_0 \). Hence \( y_1 = z_0 y_2 \) and \( \gcd(D^{2\ell+1}, y_1) = 1 \).

It follows that \( \frac{y_1}{\gcd(D^{2\ell+1}, y_1)} = D^{2\ell+1} \).

We now consider order \((x_1, D^{2\ell+1})\). If \( D \) is odd, then we claim that order \((x_1, D^{2\ell+1}) = \text{order}(x_0, D)\), equivalently, \( x_1 \equiv 1 \pmod{D^{2\ell+1}} \) if and only if \( x_0 \equiv 1 \pmod{D} \). Indeed, if \( x_1 \equiv 1 \pmod{D^{2\ell+1}} \), then by Theorem 3 (ii) we have \( x^2 - D^{2\ell+1} y^2 = 2 \) is solvable. Thus \( x^2 - D y^2 = 2 \) is also solvable and hence \( x_0 \equiv 1 \pmod{D} \). Conversely, suppose \( x_0 \equiv 1 \pmod{D} \). Since from the proof of Lemma 5, we have
\[
x_1 = \sum_{0 \leq j \leq M/2} \binom{M}{2j} x_0^{M-2j} y_0^j D^j = x_0^M \pmod{D}
\]
with \( M = \frac{D^\ell}{\gcd(D^\ell, y_0)} \) or \( M = \frac{D^\ell}{3^{\min(\ell, \ell_1)-1} \gcd(D^\ell, y_0)} \), so \( x_1 \equiv 1 \pmod{D} \). Note that \( x_1 \) is a solution of the congruence equation \( x_1 \equiv 1 \pmod{D^{2\ell+1}} \). For any odd prime \( p \) such that \( p \nmid D \), \( x_1 \) is a solution of the congruence equation \( x_1 \equiv 1 \pmod{D^{2\ell}(p^{r+1})} \) and \( x \equiv 1 \pmod{p^r} \). In view of Theorem 5.30 of [4], we can uniquely lift \( x_1 \) from a solution of \( x^2 \equiv 1 \pmod{p^r} \) to a solution \( a \) of
\[
\begin{align*}
  x^2 &\equiv 1 \pmod{p^{r+1}} \\
  x &\equiv 1 \pmod{p^r}.
\end{align*}
\]
(4.11)

Thus, \( a \equiv 1 \pmod{p^{r+1}} \). Since \( x_1 \) is also a solution of the equations in Equation (4.11), we must also have that \( x_1 \equiv 1 \pmod{p^{r+1}} \). Inductively, \( x_1 \equiv 1 \pmod{p^{r^{(2\ell+1)}}} \).

By the Chinese remainder theorem, \( x_1 \equiv 1 \pmod{D^{2\ell+1}} \). This proves the claim.

Suppose \( D \) is even. Since \( \ell \geq 1 \), we have that \( x^2 - D^{2\ell+1} y^2 = 2 \) is not solvable by Lemma 2 because \( D \neq 2d \) with odd \( d \). Hence \( x_1 \not\equiv 1 \pmod{D^{2\ell+1}} \) and so order \((x_1, D^{2\ell+1}) = 2 \).

Therefore
\[
g(D^{2\ell+1}) = \begin{cases} 
\text{lcm} \left( \text{order}(x_1, D^{2\ell+1}), \frac{D^{2\ell+1}}{\gcd(D^{2\ell+1}, y_1)} \right) & \\
\text{lcm} \left( \text{order}(x_0, D), D^{2\ell+1} \right) & \text{if } D \text{ is odd,} \\
\text{lcm} (2, D^{2\ell+1}) & \text{if } D \text{ is even,} \\
D^{2\ell+1} & \text{if } \text{order}(x_0, D) = 1 \text{ and } D \text{ is odd,} \\
2D^{2\ell+1} & \text{if } \text{order}(x_0, D) = 2 \text{ and } D \text{ is odd,} \\
D^{2\ell+1} & \text{if } D \text{ is even.}
\end{cases}
\]

This completes the proof of the theorem. \( \square \)
Corollary 4. Let $p$ be an odd prime. If $p^{\ell_0} \| y_0$, then
\[
g(p^{2\ell+1}) = \begin{cases} 
p^{2\ell+1-\min(\ell_0-\ell,2\ell+1)} & \text{if } p \equiv 7 \pmod{8}, \\
2p^{2\ell+1-\min(\ell_0-\ell,2\ell+1)} & \text{if } p \not\equiv 7 \pmod{8},
\end{cases}
\]
for $0 \leq \ell \leq \ell_0$. For $\ell > \ell_0$, we have
\[
g(p^{2\ell+1}) = \begin{cases} 
p^{2\ell+1} & \text{if } p \equiv 7 \pmod{8}, \\
2p^{2\ell+1} & \text{if } p \not\equiv 7 \pmod{8}.
\end{cases}
\]

In many of the proofs found in this section, we considered the binomial expansion of
\[
(x_0 + y_0 \sqrt{D})^n = x_n + y_n \sqrt{D}
\]
for various $n \geq 1$ in order to establish congruence properties for $x_n$ and $y_n$ modulo $D$. We now touch upon a potential alternative method to obtain the same results. We define
\[
x_{-1} = 2, \quad y_{-1} = 0, \quad u_n = \frac{y_n}{y_0}, \quad v_n = 2x_n.
\]
It is known that $x_n$, $y_n$, $u_n$, and $v_n$ are Lucas sequences, satisfying
\[
\sigma_n = 2x_1\sigma_{n-1} - \sigma_{n-2}
\]
for all $n > 0$, where $\sigma$ is any of $x, y, u, v$. There are many divisibility properties known about Lucas sequences. For some of the many identities known for $x_n, y_n, u_n, v_n$, see [10].

For certain $D$, perhaps it is possible to determine $\gcd(y_0, D)$, thus simplifying the formula for $g(D)$ given in Theorem 1. Of course, a proof of the AAC and Mordell conjectures would resolve the case for prime $D$. A related notion is the rank of apparition of $k$ in $\{y_n\}$, which is to say the smallest $n$ such that $k \mid y_n$, around which there is much literature. In the same vein, we have the following result due to Lehmer (Theorem 7 in [10] and Theorem 2.2 in [11]):

Let $p \mid D$ be prime. Then $p \nmid y_0$ if and only if
\[
\prod_{i=0}^{p-2} y_i \equiv -\left(\frac{x_0}{p}\right) \pmod{p}.
\]
This is a potentially useful result for proving more explicit versions of Theorem 1 for certain $D$.

References


Table 1: $3 \leq D \leq 100$, and $D$ is not a perfect square and $g(D) = 2D$
<table>
<thead>
<tr>
<th>$D$</th>
<th>Fundamental Solution Order</th>
<th>order($x_0, D$)</th>
<th>$g(D)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>$5 + 2\sqrt{6}$</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>$8 + 3\sqrt{7}$</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>$3 + \sqrt{8}$</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>10</td>
<td>$19 + 6\sqrt{10}$</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>18</td>
<td>$17 + 4\sqrt{4.6}$</td>
<td>2</td>
<td>18</td>
</tr>
<tr>
<td>22</td>
<td>$197 + 42\sqrt{22}$</td>
<td>2</td>
<td>22</td>
</tr>
<tr>
<td>23</td>
<td>$24 + 5\sqrt{23}$</td>
<td>1</td>
<td>23</td>
</tr>
<tr>
<td>24</td>
<td>$5 + \sqrt{24}$</td>
<td>2</td>
<td>24</td>
</tr>
<tr>
<td>26</td>
<td>$51 + 10\sqrt{26}$</td>
<td>2</td>
<td>26</td>
</tr>
<tr>
<td>30</td>
<td>$11 + 2\sqrt{4.9}$</td>
<td>2</td>
<td>30</td>
</tr>
<tr>
<td>31</td>
<td>$1520 + 273\sqrt{31}$</td>
<td>1</td>
<td>31</td>
</tr>
<tr>
<td>32</td>
<td>$17 + 3\sqrt{32}$</td>
<td>2</td>
<td>32</td>
</tr>
<tr>
<td>38</td>
<td>$37 + 6\sqrt{38}$</td>
<td>2</td>
<td>38</td>
</tr>
<tr>
<td>40</td>
<td>$19 + 3\sqrt{40}$</td>
<td>2</td>
<td>40</td>
</tr>
<tr>
<td>42</td>
<td>$13 + 2\sqrt{42}$</td>
<td>2</td>
<td>42</td>
</tr>
<tr>
<td>47</td>
<td>$48 + 7\sqrt{47}$</td>
<td>1</td>
<td>47</td>
</tr>
<tr>
<td>48</td>
<td>$7 + \sqrt{48}$</td>
<td>2</td>
<td>48</td>
</tr>
<tr>
<td>50</td>
<td>$99 + 14\sqrt{50}$</td>
<td>2</td>
<td>50</td>
</tr>
<tr>
<td>58</td>
<td>$19603 + 2574\sqrt{58}$</td>
<td>2</td>
<td>58</td>
</tr>
<tr>
<td>66</td>
<td>$65 + 8\sqrt{66}$</td>
<td>2</td>
<td>66</td>
</tr>
<tr>
<td>71</td>
<td>$3480 + 413\sqrt{71}$</td>
<td>1</td>
<td>71</td>
</tr>
<tr>
<td>74</td>
<td>$3699 + 430\sqrt{74}$</td>
<td>2</td>
<td>74</td>
</tr>
<tr>
<td>79</td>
<td>$80 + 9\sqrt{79}$</td>
<td>1</td>
<td>79</td>
</tr>
<tr>
<td>80</td>
<td>$9 + \sqrt{80}$</td>
<td>2</td>
<td>80</td>
</tr>
<tr>
<td>82</td>
<td>$163 + 18\sqrt{82}$</td>
<td>2</td>
<td>82</td>
</tr>
<tr>
<td>86</td>
<td>$10405 + 1122\sqrt{86}$</td>
<td>2</td>
<td>86</td>
</tr>
<tr>
<td>88</td>
<td>$197 + 21\sqrt{88}$</td>
<td>2</td>
<td>88</td>
</tr>
<tr>
<td>90</td>
<td>$19 + 2\sqrt{90}$</td>
<td>2</td>
<td>90</td>
</tr>
<tr>
<td>96</td>
<td>$49 + 5\sqrt{96}$</td>
<td>2</td>
<td>96</td>
</tr>
</tbody>
</table>

Table 2: $2 \leq D \leq 100$, and $D$ is not a perfect square and $g(D) = D$
<table>
<thead>
<tr>
<th>$D$</th>
<th>Fundamental Solution Order</th>
<th>$\text{order}(x_0, D)$</th>
<th>$g(D)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$3 + 2\sqrt{2}$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>$7 + 2\sqrt{12}$</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>14</td>
<td>$15 + 4\sqrt{14}$</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>20</td>
<td>$9 + 2\sqrt{20}$</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>28</td>
<td>$127 + 24\sqrt{28}$</td>
<td>2</td>
<td>14</td>
</tr>
<tr>
<td>34</td>
<td>$35 + 6\sqrt{34}$</td>
<td>1</td>
<td>17</td>
</tr>
<tr>
<td>44</td>
<td>$199 + 30\sqrt{44}$</td>
<td>2</td>
<td>22</td>
</tr>
<tr>
<td>52</td>
<td>$649 + 90\sqrt{52}$</td>
<td>2</td>
<td>26</td>
</tr>
<tr>
<td>56</td>
<td>$15 + 2\sqrt{56}$</td>
<td>2</td>
<td>28</td>
</tr>
<tr>
<td>60</td>
<td>$31 + 4\sqrt{60}$</td>
<td>2</td>
<td>30</td>
</tr>
<tr>
<td>62</td>
<td>$63 + 8\sqrt{62}$</td>
<td>1</td>
<td>31</td>
</tr>
<tr>
<td>68</td>
<td>$33 + 4\sqrt{68}$</td>
<td>2</td>
<td>34</td>
</tr>
<tr>
<td>72</td>
<td>$17 + 2\sqrt{72}$</td>
<td>2</td>
<td>36</td>
</tr>
<tr>
<td>76</td>
<td>$57799 + 6630\sqrt{76}$</td>
<td>2</td>
<td>38</td>
</tr>
<tr>
<td>92</td>
<td>$1151 + 120\sqrt{92}$</td>
<td>2</td>
<td>46</td>
</tr>
<tr>
<td>94</td>
<td>$2143295 + 221064\sqrt{94}$</td>
<td>1</td>
<td>47</td>
</tr>
<tr>
<td>98</td>
<td>$99 + 10\sqrt{98}$</td>
<td>1</td>
<td>49</td>
</tr>
</tbody>
</table>

Table 3: $2 \leq D \leq 100$, and $D$ is not a perfect square and $g(D) = D/2$

<table>
<thead>
<tr>
<th>$D$</th>
<th>Fundamental Solution Order</th>
<th>$\text{order}(x_0, D)$</th>
<th>$g(D)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>46</td>
<td>$24335 + 3588\sqrt{46}$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>54</td>
<td>$485 + 66\sqrt{54}$</td>
<td>2</td>
<td>18</td>
</tr>
<tr>
<td>70</td>
<td>$251 + 30\sqrt{70}$</td>
<td>2</td>
<td>14</td>
</tr>
<tr>
<td>78</td>
<td>$53 + 6\sqrt{78}$</td>
<td>2</td>
<td>26</td>
</tr>
<tr>
<td>84</td>
<td>$55 + 6\sqrt{84}$</td>
<td>2</td>
<td>14</td>
</tr>
</tbody>
</table>

Table 4: $2 \leq D \leq 100$, and $D$ is not a perfect square and $g(D) < D/2$