Primitive Divisors of Certain Elliptic Divisibility Sequences

Minoru Yabuta

CONTENTS
1. Introduction
2. Proof of Theorem 1.1
3. Proof of Theorem 1.2
4. Proof of Theorem 1.3
5. The Diophantine Equation $y^2 = x^3 - 2^n$
6. The Diophantine Equation $y^2 = x^3 + 3^n$
Acknowledgments
References

2000 AMS Subject Classification: 11D61, 11D25, 11G05, 11D45
Keywords: Elliptic divisibility sequence, primitive divisor, Diophantine equation

Let $E : y^2 = x^3 + D$ be an elliptic curve, where $D$ is an integer that contains no primes $p$ with $6 \mid \text{ord}_p D$. For a nontorsion rational point $P$ on $E$, write $x(nP) = A_n(P)/B_n^2(P)$ in lowest terms. We prove that for the sequence $\{B_{2m}(P)\}_{m \geq 0}$, the term $B_{2m}(P)$ has a primitive divisor for all $m \geq 3$. As an application, we give a new method for solving the Diophantine equation $y^2 = x^3 + d^n$ under certain conditions.

1. INTRODUCTION

Let $C : y^2 = x^3 + ax + b$ be an elliptic curve with integer coefficients. We denote by $C(\mathbb{Q})$ the additive group of all rational points on the curve $C$. Let $P \in C(\mathbb{Q})$ be a nontorsion point. Write

$$x(nP) = \frac{A_n(P)}{B_n^2(P)}$$

in lowest terms with $A_n(P) \in \mathbb{Z}$ and $B_n(P) \in \mathbb{N}$. The sequence $\{B_n(P)\}_{n \geq 1}$ is known as an elliptic divisibility sequence. A prime $q$ is a primitive divisor for the term $u_n$ of an integer sequence $\{u_n\}_{n \geq 1}$ if $q$ divides $u_n$ but does not divide $u_k$ for any $0 < k < n$.

M. Ward [Ward 48] first studied the arithmetic properties of elliptic divisibility sequences. Silverman [Silverman 88] was the first to show that for all sufficiently large integers $n$, the term $B_n(P)$ has a primitive divisor. Everest, Mclaren, and Ward [Everest et al. 06] obtained a uniform and quite small bound beyond which a primitive divisor is guaranteed for congruent number curves $E_T : y^2 = x^3 - T^2x$ with $T > 0$ square-free. Improving their work, Ingram [Ingram 07] showed that for the curve $E_T$, if $5 \mid n$ or $n > 2$ is even, then $B_n(P)$ has a primitive divisor, and furthermore, if $x(P) < 0$ or $\{x(P), x(P) + T, x(P) - T\}$ contains a rational square, then $B_n(P)$ has a primitive divisor for all $n > 2$.

The main purpose of this paper is to prove the following theorems. For a rational number $r \neq 0$ we write
Theorem 1.1. Let \( E : y^2 = x^3 + D \) be an elliptic curve, where \( D \) is an integer that contains no primes \( q \) with \( 6 \mid \ord_q D \), and assume that \( E \) has a nontorsion rational point \( P \). Then for the elliptic divisibility subsequence \( \{ B_{2n}(P) \}_{n \geq 0} \), the term \( B_{2n}(P) \) has a primitive divisor for all integers \( n \geq 3 \).

Theorem 1.2. Let \( C : y^2 = x^3 + Ax \) be an elliptic curve, where \( A \) is an integer that contains no primes \( q \) with \( 4 \mid \ord_q A \), and assume that \( C \) has a nontorsion rational point \( P \). Then for the elliptic divisibility subsequence \( \{ B_{2n}(P) \}_{n \geq 0} \), the term \( B_{2n}(P) \) has a primitive divisor for all integers \( n \geq 3 \).

These bounds in Theorems 1.1 and 1.2 are sharp. The proofs are elementary. However, our results are significant because the duplication map plays a very important role in the arithmetic of elliptic curves. Unfortunately, we do not work for other Weierstrass curves in minimal form. We anticipate that Theorems 1.1 and 1.2 might be generalized by other methods.

We next give a new method for solving the Diophantine equation \( y^2 = x^3 + d^n \) in the integer variables \( x, y \), and \( n \) under certain conditions. We call an integral solution \((x, y)\) trivial if \( xy = 0 \), and primitive if \( \gcd(x, y) = 1 \). We can write \( n = 6m + r \) with \( 0 \leq r < 6 \). Applying Theorem 1.1, we obtain the following theorem.

Theorem 1.3. Let \( r \) be an integer with \( 0 \leq r < 6 \), and let \( d \) be an even integer that is sixth-power-free. Let \( E_m : y^2 = x^3 + d^{4m+r} \) be an elliptic curve, and assume that \( E_0 : y^2 = x^3 + d^r \) has rank one. If \( E_N \) has a nontrivial primitive integral point, then \( E_m \) has no nontrivial primitive integral points for any integer \( m \geq N + 3 \).

In 1977, using algebraic number theory, Rabinowitz [Rabinowitz 77] gave the full set of integer solutions to the Diophantine equations \( y^2 = x^3 + 2^n \). As an application of Theorem 1.3, we will give a new method for solving the equations \( y^2 = x^3 + 2^n \). Our method is geometric. We anticipate that our results might find other applications.

Primitive divisors have been studied by many authors. A Lucas sequence is defined by \( U_n = (\alpha^n - \beta^n) / (\alpha - \beta) \), where \( \alpha + \beta \) and \( \alpha \beta \) are coprime nonzero integers and the quotient of \( \alpha \) and \( \beta \) is not a root of unity. In 1892, Zsigmondy [Zsigmondy 92] showed that for the sequence \( u_n = a^n - b^n \), the term \( u_n \) has a primitive divisor for all \( n > 6 \), where \( a \) and \( b \) are positive coprime integers.

In 1913, Carmichael [Carmichael 13] showed that if \( \alpha \) and \( \beta \) are real, then \( U_n \) has a primitive divisor for all \( n > 12 \). Ward [Ward 55] and Durst [Durst 59] extended Carmichael’s result to Lehmer sequences. In 1974, Schinzel [Schinzel 74] proved that there exists an effectively computable constant \( N \) independent of \( \alpha \) and \( \beta \) such that \( U_n \) has a primitive divisor for all \( n > N \) provided \( \alpha \) and \( \beta \) are complex. In 1977, Stewart [Stewart 77] showed that if \( n > e^{452} 2^{67} \), then \( U_n \) has a primitive divisor. In 1998, Voutier [Voutier 98] proved that if \( n > 30030 \), then the \( n \)th term of any Lucas or Lehmer sequence has a primitive divisor. In 2001, Bilu, Hanrot, and Voutier [Bilu et al. 01] obtained a major result for Lucas and Lehmer sequences. They proved that if \( n > 30 \), then every \( m \)th Lucas and Lehmer number has a primitive divisor, and they listed all Lucas and Lehmer numbers without a primitive divisor.

In the same paper, Bilu et al. linked the existence of primitive divisors for Lucas and Lehmer numbers with Thue equations of high degree. Traditionally, primitive divisor theory has been associated with Diophantine equations. Our approach follows the classical path. We also link the existence of primitive divisors for elliptic divisibility sequences with resolving an important class of Diophantine equations.

2. PROOF OF THEOREM 1.1

In this section, we consider an elliptic curve \( E : y^2 = x^3 + D \), where \( D \) is a nonzero integer that contains no primes \( q \) with \( 6 \mid \ord_q D \). Assume that \( E \) has a nontorsion rational point \( P \). Write \( x(nP) = A_n(P) / B_n^2(P) \) in lowest terms with \( A_n(P) \in \mathbb{Z} \) and \( B_n(P) \in \mathbb{N} \). The sequence \( \{ B_n(P) \}_{n \geq 1} \) is a divisibility sequence, which means that \( B_m(P) \mid B_n(P) \) whenever \( m \mid n \). For \( P \in E(\mathbb{Q}) \) we write \( P = (u/\ell^2, v/\ell^3) \) in lowest terms. Then by the duplication formulas we obtain

\[
x(2P) = \frac{u(u^3 - 8D \ell^6)}{4v^2 \ell^2} = \frac{u(9u^3 - 8v^2)}{4v^2 \ell^2},
\]

\[
y(2P) = \frac{v^6 + 20D^2u^3e^6 - 8D^2e^{12}}{8u^3 \ell^3} = \frac{-27u^6 + 36u^3v^2 - 8v^4}{8u^3 \ell^3}.
\]

We use the following standard notation: if \( p \) is a prime, we write \( p^k \parallel m \) to indicate that \( p^k \) is the highest power of \( p \) dividing \( m \).
Lemma 2.1. For \( P \in E(\mathbb{Q}) \) write \( P = (u/e, v/e^3) \) and \( 2^n P = (u_n/e_n^n, v_n/e_n^n) \) in lowest terms. If \( u \) and \( v \) are coprime, then \( v_n \) is odd, not divisible by 3, and prime to \( u_n \) for all integers \( n \geq 1 \).

Proof: Put \( U = u(9u^3 - 8v^2), \ V = -27u^6 + 36u^3v^2 - 8v^4 \).

If \( u \equiv 0 \pmod{p} \), then \( U \equiv 0 \pmod{p} \). If \( u \equiv 0 \pmod{p} \), then \( U \equiv 0 \pmod{p} \).

We will prove that \( u_n \) and \( v_n \) are coprime. The proof is by contradiction. Suppose that \( u_1 = v_1 = 0 \pmod{p} \) for some prime \( p \). Since \( v_1 \) is odd and not divisible by 3, we may assume that \( p \geq 5 \). We have

\[
\begin{align*}
U &= u(9u^3 - 8v^2) \equiv 0 \pmod{p}, \quad (2-1) \\
-27u^6 + 36u^3v^2 - 8v^4 &\equiv 0 \pmod{p}, \quad (2-2)
\end{align*}
\]

If \( u \equiv 0 \pmod{p} \), then from \( (2-2) \) we have \( U \equiv 0 \pmod{p} \).

If \( u \equiv 0 \pmod{p} \), then \( U \equiv 0 \pmod{p} \).

Thus we obtain that 3 divides \( u_n \) in lowest terms, where \( s_n \) and \( t_n \) are prime to \( p \). Put \( \nu_n = 3k_n - 2l_n \) and

\[
T_{n+1} = -27p^{2\nu_n}s_n^6 + 36p^{2\nu_n}s_n^3t_n^2 - 8t_n^4.
\]

Assume that \( s \) and \( t \) are coprime. Then for all integers \( n \geq 1 \),

1. \( t_n \) is odd, not divisible by 3, and prime to \( s_n \).
2. \( 3p^{\nu_n} \) is an integer, and \( t_{n+1} = T_{n+1} \) or \( 2^{-3}T_{n+1} \).

Proof: Put \( \nu = 3k - 2l \). By duplication formulas we obtain that

\[
\begin{align*}
x(2P) &= \frac{p^k s(9p^{\nu}s^3 - 8t^2)}{4t^2e^2}, \\
y(2P) &= \frac{p^l(-27p^{2\nu}s^6 + 36p^{2\nu}s^3t^2 - 8t^4)}{8t^3e^3}.
\end{align*}
\]

We put \( S_{n+1} = s_n(9p^{\nu_n}s_n^3 - 8t_n^2) \).

1. A similar argument to that in the proof of Lemma 2.1 would show that \( t_n \) is odd not divisible by 3 and prime to \( s_n \).
2. We distinguish three cases.

Case 1. Let \( p \geq 5 \). If \( \nu \) is positive then \( k_1 = k \) and \( l_1 = l \), so \( v_1 \) is also positive. If \( \nu \) is negative then \( k_1 = k + \nu \) and \( l_1 = l + 2\nu \), so \( v_1 \) is zero. Assume that \( \nu \) is zero. Then we can write \( k = 2m \) and \( l = 3m \) for some positive integer \( m \).

If we let \( x = p^{2m}s/e^2 \) and \( y = p^{3m}/e^3 \), then the equation \( y^2 = x^3 + D \) becomes \( p^{6m}(t^2 - s^3) = D e^6 \). From our assumption \( 4 \mid \text{ord}_p D \), we have that \( \text{ord}_p D > 6m \), so we must have \( t^2 - s^3 \equiv 0 \pmod{p} \). Then \( S_1 \equiv s^6 \not\equiv 0 \pmod{p} \) and \( T_1 \equiv s^6 \not\equiv 0 \pmod{p} \). Therefore \( k_1 = 2m \) and \( l_1 = 3m \), and hence \( v_1 \) is zero.

Case 2. Let \( p = 2 \). Then

\[
x(2P) = \frac{2^k s(9 \cdot 2^{-2-3} s^3 - 2t^2)}{4t^2e^2}, \\
y(2P) = \frac{2^l(-27 \cdot 2^{2-3} s^6 + 9 \cdot 2^{-1} s^3 t^2 - t^4)}{8t^3e^3}
\]

If \( \nu \geq 2 \) then \( k_1 \geq k \) and \( l_1 = l \); therefore \( v_1 \geq 2 \). If \( \nu < 2 \) then \( k_1 = k + \nu - 2 \) and \( l_1 = l + 2\nu - 3 \); therefore \( v_1 \) is zero.

Case 3. Let \( p = 3 \). Then

\[
x(2P) = \frac{3^k s(3 \cdot 3^{\nu} s^3 - 8t^2)}{4t^2e^2}, \\
y(2P) = \frac{3^l(-27 \cdot 3^{2\nu} s^6 + 36 \cdot 3^{2\nu} t^2 - 8t^4)}{8t^3e^3}
\]

If \( \nu \geq 0 \) then \( k_1 = k \) and \( l_1 = l \); therefore \( v_1 \geq \nu \). If \( \nu \leq -2 \) then \( k_1 \geq k + \nu + 2 \) and \( l_1 = l + 2\nu + 3 \); therefore \( v_1 \geq 0 \). If \( \nu = -1 \) then \( k_1 = k \) and \( l_1 = l \); therefore \( v_1 = \nu = -1 \).

Thus we obtain that \( 3p^{\nu_n} \) is an integer. Next we will show that \( t_2 = T_2 \) or \( 2^{-3}T_2 \). As mentioned before, \( t_1 \) is an odd integer not divisible by 3 and prime to \( s_1 \). So if \( p \geq 3 \) and \( 2 \mid s_1 \) or if \( p = 2 \) and \( \nu_1 \geq 2 \), then \( 2^2 \mid T_2 \). Otherwise, \( T_2 \) is odd. A similar argument to that in Lemma 2.1 gives that \( S_2 \) and \( T_2 \) have no common prime divisors larger than 2. It follows that \( t_2 \) is equal to \( T_2 \) or \( 2^{-3}T_2 \).

Using induction gives the desired result.

Now we are ready to prove Theorem 1.1.

Proof of Theorem 1.1: Let \( P \) be a non-torsion rational point on the curve \( E \), and let \( n \geq 1 \) be an arbitrary positive integer. Write \( 2^n P = (a_n/s_n^n, b_n/t_n^n) \) in lowest terms with \( e_n > 0 \), where \( a_n \) and \( b_n \) have the factorizations \( a_n = p_{1n}^{\alpha_1}p_{2n}^{\alpha_2} \cdots p_{m_n}^{\alpha_m} \) and \( b_n = p_{1n}^{\beta_1}p_{2n}^{\beta_2} \cdots p_{m_n}^{\beta_m} \), and \( \gcd(s_n, t_n) = \gcd(s_n, a_n) = \gcd(t_n, b_n) = 1 \). Let
c_n = a^3_n b^{-2}. Then c_n = p_1^{\nu_1} p_2^{\nu_2} \cdots p_m^{\nu_m}, where \nu_i = 3 \alpha_i - 2 \beta_i. From Lemma 2.2 we have that 3c_n is an integer. As mentioned in the proof of Lemma 2.2, the hypothesis that there are no primes q with 6 \mid \text{ord}_D is used to show that \nu_i \geq 0, provided p_i \geq 5. By the duplication formulas we obtain
\[
x(2^{n+1}P) = \frac{a_n s_n (9c_n s_n^3 - 8t_n^2)}{4t_n^2 e_n^2},
\]
\[
y(2^{n+1}P) = \frac{b_n (-27c_n s_n^6 + 36c_n s_n^3 t_n - 8t_n^4)}{8t_n^3 c_n e_n^4}.
\]
From Lemma 2.2 we see that \(t_n\) is odd, not divisible by 3, and prime to \(s_n\) for all \(n \geq 1\). So to prove that the denominator of \(x(2^{n+2}P)\) has a primitive divisor, it suffices to show that \(t_n+1 \neq \pm 1\). Now put
\[
T_{n+1} = -27c_n s_n^6 + 36c_n s_n^3 t_n - 8t_n^4. \quad (2-3)
\]
Then from Lemma 2.2 we have that \(T_{n+1} = T_{n+1} + 1\) or \(-3T_{n+1}\).

We will now prove that \(T_{n+1} = T_{n+1} + 1\) or \(-3T_{n+1}\).

Using SIMATH, we can solve the Diophantine equation \(y^2 = x^3 - 36x\). All integer solutions are as follows: \((x, y) = (\pm 6, 0), (\pm 3, \pm 9), (\pm 2, \pm 8), (0, 0), (12, 36), (18, \pm 72), (294, \pm 5040)\). So \((12t_n, 36t_n w_n) = (12, 36), \) and therefore \(t_n \equiv 1\). Substituting this and \(T_{n+1} = 1\) into (2-4), we obtain \(c_n s_n^3 = 1\). Therefore \(c_n = 1\) and \(s_n = 1\). Hence
\[
2^n P = \left( \frac{a_n}{e_n^2}, \frac{b_n}{e_n^3} \right), \quad 2^{n+1} P = \left( \frac{a_n}{4e_n^2}, \frac{b_n}{8e_n^3} \right).
\]
The points \(2^n P\) and \(2^{n+1} P\) lie on the curve \(y^2 = x^3 + D\). Therefore
\[
b_n^2 = a_n^3 + Dc_n^6 \quad \text{and} \quad b_n^2 = a_n^3 + 64Dc_n^6.
\]
This is impossible. Hence \(T_{n+1} \neq 1\).

**Case 3.** Suppose that \(T_{n+1} = 2^3\). Reducing the equation \(4t_n^4 - 2^3 = 3w_n^2\) modulo 3, we obtain the congruence \(4t_n^4 - 2^3 \equiv 0 \mod 3\). But this congruence has no solutions. Hence \(T_{n+1} \neq 2^3\).

**Case 4.** Suppose that \(T_{n+1} = -2^3\). Then we have that \(4t_n^4 + 2^3 = 3w_n^2\). Putting \(X = 12t_n^2\) and \(Y = 36t_n w_n\), we have
\[
Y^2 = X^3 + 288X.
\]
By SIMATH, all integer solutions of the equation \(y^2 = x^3 + 288x\) are as follows: \((x, y) = (0, 0), (1, \pm 7), (12, \pm 72), (24, \pm 144), (288, \pm 4896)\). So \((12t_n, 36t_n w_n) = (0, 0), (12, 72), \) and therefore \(t_n = 0\) or \(\pm 1\). Then from (2-4) we have \(9c_n s_n^3 = 12\), which is impossible. Hence \(T_{n+1} \neq -2^3\). We have thus completed the proof.

**Remark 2.3.** The bound of Theorem 1.1 is sharp. For example, if \(E : y^2 = x^3 + 80P = (4, 12)\) is a nontorsion point on \(E\), then \(2P = (-4, 4)\) and \(2^2 P = (44, -292)\).

**3. PROOF OF THEOREM 1.2**

The proof of Theorem 1.2 is a slight variant of that of Theorem 1.1. In this section we consider an elliptic curve \(C : y^2 = x^3 + Ax\), where \(A\) is an integer that contains no primes \(q\) with \(4 \mid \text{ord}_D\). Assume that the curve \(C\) has a nontorsion rational point \(P\). If we let \(P = (x, y)\), then by the duplication formulas we obtain
\[
x(2P) = \frac{(x^2 - A)^2}{4y^2} = \frac{(y^2 - 2x^3)^2}{4x^2 y^2},
\]
\[
y(2P) = \frac{x^6 + 54x^4 y^2 - 5A^2 y^2 - A^3}{8y^3} = \frac{(y^2 - 2x^3)(4x^6 - 4x^4 y^2 - y^4)}{8x^3 y^3}.
\]
We can write \(P = (bu^2/c^2, av/c^3)\) in lowest terms, where \(u\) and \(v\) are coprime; see [Silverman and Tate 94].

**Lemma 3.1.** Let \(P \in C(Q)\) be of the form \((u^2/c^2, uv/c^3)\) in lowest terms with gcd\((u, v) = 1\). Then \(2^n P\) has the form \((u_n^2/c_n^2, u_n v_n/c_n^3)\) in lowest terms, where \(u_n\) and \(v_n\) are odd and coprime for all integers \(n \geq 1\).

**Proof:** By duplication formulas we obtain that
\[
x(2P) = \frac{(u^2 - 2u^4)^2}{4u^2 v^2 c^2},
\]
\[
y(2P) = \frac{(v^2 - 2u^4)(4u^8 - 4u^4 v^2 - v^4)}{8u^3 v^3 c^3}.
\]
Put \(U_1 = v^2 - 2u^4\) and \(V_1 = 4u^8 - 4u^4 v^2 - v^4\). If \(v\) is odd, then \(U_1\) and \(V_1\) are odd, while \(v\) is even, then
2 \parallel U_1 and 2^2 \parallel V_1. Therefore both \( u_1 \) and \( v_1 \) are odd. A similar argument to that in Lemma 2.1 would show that \( u_1 \) and \( v_1 \) are coprime. Using induction gives the desired result.

**Lemma 3.2.** Let \( p \) be a prime, and let \( P = (p^k s^2/e^2, \ y \ s t/e^3) \in C(\mathbb{Q}) \) be in lowest terms with \( k > 0, l > 0, \) and \( \gcd(s, t) = \gcd(s, p) = \gcd(t, p) = 1. \) Then \( 2^m P \) has the form \( (p^{4m} s^2/e^2, \ p^{3m} st/e^3) \) in lowest terms with \( \gcd(s, n, p) = \gcd(t, n, p) = 1 \) for all \( n \geq 1. \) Put \( n = 3k - 2t. \) Then for all integers \( n \geq 1, \)

1. \( s_n \) and \( t_n \) are odd coprime integers.
2. \( s_{n+1} = t_n^2 - 2p^n s_n^4 \) and \( t_{n+1} = 4p^{2m} s_n^8 - 4p^n s_n^4 t_n^2 - t_n^4. \)

**Proof:** If we put \( \nu = 3k - 2l, \) then

\[
x(2P) = \frac{p^{k-\nu}(t^2 - 2p^n s^4)^2}{4s^2 t^2 e^2},
\]

\[
y(2P) = \frac{p^{l-\nu}(t^2 - 2p^n s^4)}{8s^3 t^3 e^3}.
\]

Put \( S_1 = t^2 - 2p^n s^4 \) and \( T_1 = 4p^{2m} s_n^8 - 4p^n s_n^4 t_n^2 - t_n^4. \)

(1) The proof is similar to that for Lemma 3.1, so we omit it.

(2) We will show that \( v_1 \) is nonnegative. We distinguish two cases.

**Case 1.** Let \( p \geq 3. \) If \( \nu \) is positive then \( k_1 = k - \nu \) and \( l_1 = l - \nu; \) therefore \( v_1 \) is zero. If \( \nu \) is negative then \( k_1 = k + \nu \) and \( l_1 = l + 2\nu; \) therefore \( v_1 \) is zero. Assume that \( \nu \) is zero. Then we can write \( k = 2m \) and \( l = 3m \) for some positive integer \( m. \) If we let \( x = p^{2m} s^2/e^2 \) and \( y = p^{3m} st/e^3, \) then the equation \( y^2 = x^3 + Ax \) becomes \( p^{4m}(t^2 - s^4) = Ax^4. \) From our assumption \( 4 \nmid \ord_A, \) we have that \( \ord_A > 4. \) Therefore we must have \( t^2 - s^4 \equiv 0 \pmod{p}. \) We obtain \( S_1 \equiv -s^4 \not\equiv 0 \pmod{p} \) and \( T_1 \equiv -s^8 \not\equiv 0 \pmod{p}. \) Therefore \( k_1 = k = 2m \) and \( l_1 = 3m, \) and hence \( v_1 \) is zero.

**Case 2.** Let \( p = 2. \) Then

\[
x(2P) = \frac{2^{k-\nu}(t^2 - 2^{\nu+1}s^4)}{s^2 t^2 e^2},
\]

\[
y(2P) = \frac{2^{l-\nu}(t^2 - 2^{\nu+1}s^4)}{8s^3 t^3 e^3},
\]

If \( \nu \geq 0 \) then \( k_1 = k - \nu - 2 \) and \( l_1 = l - \nu - 3; \) therefore \( v_1 \) is zero. If \( \nu \leq -2 \) then \( k_1 = k + \nu \) and \( l_1 = l + 2\nu; \) therefore \( v_1 \) is zero. Assume that \( \nu = -1. \) Then

\[
x(2P) = \frac{2^{k-1}(t^2 - s^4)^2}{s^2 t^2 e^2},
\]

\[
y(2P) = \frac{2^{l-2}(t^2 - s^4)(s^8 - 2s^4 t^2 - t^4)}{8s^3 t^3 e^3}.
\]

Put \( S_1 = t^2 - s^4 \) and \( T_1 = s^8 - 2s^4 t^2 - t^4. \) Since \( s \) and \( t \) are odd, we have \( 2 \parallel T_1 \) and \( 2^2 \parallel S_1 \) for some integer \( r \geq 2. \) Therefore \( k_1 = k + 2r - 1 \) and \( l_1 = l + r - 1, \) and hence \( v_1 = 4r - 1 > 0. \)

It follows that \( v_1 \) is nonnegative. We put

\[
S_2 = t_1^2 - 2p^n s_1^4 \quad \text{and} \quad T_2 = 4p^{2m} s_1^8 - 4p^n s_1^4 t_1^2 - t_1^4. \]

Here \( s_1 \) and \( t_1 \) are odd and coprime, so an argument similar to that for Lemma 2.1 would show that \( S_2 \) and \( T_2 \) are odd coprime integers and both of them are prime to \( p. \) Hence \( s_2 = S_2 \) and \( t_2 = T_2. \) Using induction gives the desired result.

**Proof of Theorem 1.2:** Let \( P \) be a nontorsion rational point on the curve \( C: y^2 = x^3 + Ax, \) and let \( n \geq 1 \) be an arbitrary positive integer. Write \( 2^m P = (a_n s_n^2/e_n, b_n s_n t_n/e_n) \) in lowest terms with \( e_n > 0, \) where \( a_n \) and \( b_n \) have the factorizations \( a_n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \) and \( b_n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m}, \) and \( \gcd(s_n, t_n) = \gcd(n, a_n) = \gcd(t_n, b_n) = 1. \) Then \( c_n = a_n b_n. \) Then \( c_n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}, \) where \( \nu_i = 3\alpha_i - 2\beta_i. \) From Lemma 3.2 we have that \( c_n \) is an integer for all \( n \geq 1. \) As mentioned in the proof of that lemma, the hypothesis that there are no primes \( q \) with \( 4 \nmid \ord_q A \) is used to show that \( v_n \geq 0, \) provided \( p_1 \geq 3. \) By the duplication formulas we obtain

\[
x(2n+1)P = \frac{a_n c_n^{-1}(t_n^2 - 2c_n s_n^4)^2}{4s_n^2 t^2 e_n^2},
\]

\[
y(2n+1)P = \frac{b_n c_n^{-1}(t_n^2 - 2c_n s_n^4)(4c_n^2 s_n^8 - 4c_n s_n^4 t_n^2 - t_n^4)}{8s_n^3 t^3 e_n^3}.
\]

From Lemma 3.2 we observe that \( s_n \) and \( t_n \) are odd co-prime integers and

\[
s_{n+1} = t_n^2 - 2c_n s_n^4, \quad t_{n+1} = 4c_n s_n^8 - 4c_n s_n^4 t_n^2 - t_n^4.
\]

Put \( X = t_n^2 \) and \( Y = 2c_n s_n^4. \) Then

\[
s_n+1 = X - Y \quad \text{and} \quad t_n+1 = Y^2 - 2XY - X^2,
\]

and so

\[
2X^2 = s_{n+1}^2 - t_{n+1} \quad \text{and} \quad Y = X - s_{n+1}. \tag{3-1}
\]

To prove that the denominator of \( x(2n+2)P \) has a primitive divisor, it suffices to show that \( s_{n+1}t_{n+1} \neq \pm 1. \) The
proof is by contradiction. Suppose that \( s_{n+1}t_{n+1} = \pm 1 \). Then from (3–1), we have \( X = 1 \) and \( Y = 2 \), and therefore \( s_n = \pm 1 \), \( t_n = \pm 1 \), and \( c_n = 1 \). So

\[
2^n P = \left( \frac{a_n}{c_n^2}, \pm \frac{b_n}{c_n^3} \right) \quad \text{and} \quad 2^{n+1} P = \left( \frac{a_n}{4e_n^2}, \pm \frac{b_n}{8e_n^3} \right).
\]

The points \( 2^n P \) and \( 2^{n+1} P \) lie on the curve \( y^2 = x^3 + Ax \). Therefore

\[
b_n^2 = a_n^3 + Aa_ne_n^4 \quad \text{and} \quad b_n^2 = a_n^3 + 16Aa_ne_n^4.
\]

This is impossible. Hence \( s_{n+1}t_{n+1} \neq \pm 1 \). We have completed the proof. \( \square \)

Remark 3.3. The bound of Theorem 1.2 is sharp. For example, if \( C : y^2 = x^3 - 192x \) and \( P = (24,96) \) is a nontorsion point on \( C \), then \( 2P = (16,-32) \) and \( 2^2 P = (49,329) \).

4. PROOF OF THEOREM 1.3

Let \( r \) be a fixed integer with \( 0 \leq r < 6 \). Let \( E_0 : y^2 = x^3 + d^r \) be an elliptic curve, where \( d \) is a sixth-power-free even integer. For a positive integer \( k \) and the curve \( E_0 \), we define

\[
E_0(k) = \{(x,y) \in E_0(\mathbb{Q}) : k^2 \text{ divides the denominator of } x\}.
\]

The following proposition is well known (see, for example, [Cassels 91]).

Proposition 4.1. Let \( p \) be a prime. Then for every point \( P \in E_0(p) \) and every nonzero integer \( n \),

\[
\text{ord}_p x(nP) = \text{ord}_p x(P) - 2\text{ord}_p n.
\]

Lemma 4.2. If the curve \( E_0 : y^2 = x^3 + d^r \) has rank one, then \( E_0(d) \) is an infinite cyclic group.

Proof: The set \( E_0(d) \) is simply the intersection of \( E_0(p^r) \) for all prime powers \( p^r \) dividing \( d \). Each \( E_0(p^r) \) is torsion-free, so \( E_0(d) \) is torsion-free. Since \( E_0(d) \) sits inside \( \mathbb{Z} \times F \) for a finite group \( F \), it follows that \( E_0(d) \) itself is cyclic. \( \square \)

Proof of Theorem 1.3: If \( E_m : y^2 = x^3 + d^m + r \) has a nontrivial primitive integral point \((s,t)\), then \( E_0 : y^2 = x^3 + d^r \) has a rational point of the form \((s/d^m,t/d^m)\) in lowest terms. This theorem can be restated as saying that for any integer \( m \geq N + 3 \), the group \( E_0(\mathbb{Q}) \) of all rational points on the curve \( E_0 \) has no points of the form \((s/d^m,t/d^m)\) in lowest terms.

By our assumption, the curve \( E_0 \) has rank one, so from Lemma 4.2, we have that \( E_0(d) \) is an infinite cyclic group. Let \( P_0 \) be a generator for \( E_0(d) \). Assume that \( E_N \) has a nontrivial primitive integral point. Let \( k_0 \) be the least positive integer \( k \) such that \( kP_0 \) has the form \((u/d^N,v/d^N)\) in lowest terms. Then, from Theorem 1.1 we obtain that the denominator of \((s/d^m,kP_0)\) has a divisor not dividing \( d \) for all integers \( n \geq 3 \). Hence, for any nontorsion point \( P \in E_0(\mathbb{Q}) \), if the denominator of \( x(P) \) is divided by \( d^{2(N+3)} \), then it has a divisor not dividing \( d \). It follows that \( E_m \) has no nontrivial primitive integral points for any integer \( m \geq N + 3 \). \( \square \)

5. THE DIOPHANTINE EQUATION \( y^2 = x^3 - 2^n \)

As an application of Theorem 1.3, we will give a new method for solving the Diophantine equation \( y^2 = x^3 - 2^n \). The following argument is another approach to the results of [Rabinowitz 77].

All integer solutions of the equation \( y^2 = x^3 - 2^n \) for integers \( 0 \leq n \leq 5 \) are as follows:

| \( n \) | Solutions |
|-----|--------|
| 0   | (1,0)  |
| 1   | (3,±5) |
| 2   | (2,±3), (5,±11) |
| 3   | (2,0)  |
| 4   | no solutions |
| 5   | no solutions |

Lemma 5.1. Let \( n \geq 0 \) be an integer. Then the elliptic curve \( C_n : y^2 = x^3 - 2^n \) has a nontrivial primitive integral point if and only if \( n = 1,2 \).

Proof: As mentioned above, \( C_n \) has a primitive integral point for \( n = 1,2 \), and does not for \( n = 0,3,4,5 \). Now write \( n = 6m + r \) with \( 0 \leq r < 6 \). Then each of the curves \( C_0, C_3, C_4, \) and \( C_5 \) has rank zero. First we will show that \( C_{6m} \) has no primitive integral points for any \( m \geq 1 \). Suppose that the curve \( C_{6m} \) has a primitive integral point \((u,v)\). Then

\[
v^2 = u^3 - 2^{6m} \quad \text{or} \quad (v/2^{3m})^2 = (u/2^{2m})^3 - 1.
\]

The curve \( C_0 : y^2 = x^3 - 1 \) has rank zero; in other words, all rational points on \( C_0 \) are torsion. By the Nagell–Lutz theorem, a torsion point has integer coordinates. Hence \( m = 0 \). It follows that \( C_{6m} \) has no primitive integral points for any \( m \geq 1 \). Similarly, none of \( C_{6m+3}, C_{6m+4} \),...
and $C_{6m+5}$ has primitive integral points for any integer $m \geq 1$.

Both $C_1$ and $C_2$ have rank one, and $C_1(\mathbb{Q}) \simeq \langle (3, 5) \rangle$ and $C_2(\mathbb{Q}) \simeq \langle (2, 2) \rangle$. Let

$$C_n(2) = \{(x, y) \in C_n(\mathbb{Q}) : 2^2 \text{ divides the denominator of } x\}.$$  

Then $C_n(2)$ is an infinite cyclic group. Put $P = (3, 5)$. Then

$$2P = \left(\frac{129}{2^2 \cdot 5^2}, \frac{-383}{2^3 \cdot 5^3}\right),$$

and therefore $2P$ is a generator for $C_1(\mathbb{Q})$. Next put $Q = (2, 2)$. Then

$$2Q = (5, -11),$$

$$3Q = \left(\frac{106}{3^2}, \frac{1090}{3^3}\right),$$

$$2^2Q = \left(\frac{785}{2^2 \cdot 11^2}, \frac{-5497}{2^3 \cdot 11^3}\right),$$

and therefore $2^2Q$ is a generator for $C_2(\mathbb{Q})$. From Proposition 4.1, there are no rational points of the form $(u/2^{2m}, v/2^{3m})$ on $C_1$ and $C_2$ for any integer $m \geq 1$. Hence neither $C_{6m+1}$ nor $C_{6m+2}$ has primitive integral points for any integer $m \geq 1$. We have thus completed the proof.

Using this lemma, we will give all integer solutions to the equation $y^2 = x^3 - 2^n$.

**Theorem 5.2.** [Rabinowitz 77] All integer solutions of the Diophantine equation $y^2 = x^3 - 2^n$ are as follows:

| $n \mod 6$ | Solutions |
|------------|-----------|
| $n \equiv 0 \mod 6$ | $(2^m, 0)$ |
| $n \equiv 1 \mod 6$ | $(3 \cdot 2^m, \pm 5 \cdot 2^{3m})$ |
| $n \equiv 2 \mod 6$ | $(2 \cdot 2^{2m}, \pm 2 \cdot 2^{3m}), (5 \cdot 2^{2m}, \pm 11 \cdot 2^{3m})$ |
| $n \equiv 3 \mod 6$ | $(2 \cdot 2^{2m}, 0)$ |
| $n \equiv 4 \mod 6$ | no solutions |
| $n \equiv 5 \mod 6$ | no solutions |

**Proof:** We write $n = 6m + r$ with $0 \leq r < 6$. Assume that the equation $y^2 = x^3 - 2^{6m+r}$ has an integer solution $(u, v)$. Then

$$\left(\frac{u}{2^{3m}}\right)^2 = \left(\frac{v}{2^{3m}}\right)^3 - 2^r.$$  

As shown in the proof of Lemma 5.1, for all $m \geq 1$ both $u/2^{2m}$ and $v/2^{3m}$ must be integers. If $(u_0, v_0)$ is an integer solution of the equation $y^2 = x^3 - 2^r$, then $u = 2^{2m}u_0$ and $v = 2^{3m}v_0$. Thus we have completed the proof.

6. **THE DIOPHANTINE EQUATION** $y^2 = x^3 + 3^n$

In this section, we will solve the equation $y^2 = x^3 + 3^n$ by our methods.

**Lemma 6.1.** Let $n \geq 0$ be an integer. Then the elliptic curve $C_n : y^2 = x^3 + 3^n$ has no nontrivial primitive integral points for all integers $n \geq 6$.

**Proof:** All integer solutions of the equation $y^2 = x^3 + 3^n$ for integers $0 \leq n \leq 5$ are as follows:

| $n$ | Solutions |
|-----|-----------|
| 0   | $(-1, 0), (0 \pm 1), (2, \pm 3)$ |
| 1   | $(1, \pm 2)$ |
| 2   | $(0, \pm 3), (-2, \pm 1), (3, \pm 6), (6, \pm 15), (40, \pm 253)$ |
| 3   | $(-3, 0)$ |
| 4   | $(0, \pm 9)$ |
| 5   | no solutions |

Each of the curves $C_0, C_3, C_4, \text{ and } C_5$ has rank zero. By a similar argument as in the proof of Lemma 5.1, we have that none of $C_{6m}, C_{6m+3}, C_{6m+4}, C_{6m+5}$ has primitive integral points for any integer $m \geq 1$. Both $C_1$ and $C_2$ have rank one, and $C_1(\mathbb{Q}) \simeq \langle (1, 2) \rangle$ and $C_2(\mathbb{Q}) \simeq \langle (-2, 1) \rangle \oplus \langle (0, 3) \rangle$. Let

$$C_n(3) = \{(x, y) \in C_n(\mathbb{Q}) : 3^2 \text{ divides the denominator of } x\}.$$  

Put $P = (1, 2)$. Then we have

$$2P = \left(\frac{-23}{2^2}, \frac{-11}{2^5}\right), \quad 3P = \left(\frac{1873}{3^2 \times 13^2}, \frac{-130870}{3^3 \times 13^3}\right).$$

Therefore $3P$ is a generator for $C_1(3)$.

Next put $Q = (-2, 1)$ and $R = (0, 3)$. Then $R$ is a torsion point of order 3. After a little computation, we have that the denominator of $x(iQ + jR)$ is not divisible by 3 for $i = 1, 2, 3$ and $j = 1, 2,$ and

$$2Q = (40, -253), \quad 3Q = \left(\frac{-629}{3^2 \times 7^2}, \frac{22870}{3^3 \times 7^3}\right).$$

Therefore $3Q$ is a generator for $C_2(3)$. Hence from Proposition 4.1 there are no rational points of the form $(u/3^{2m}, v/3^{3m})$ on $C_1$ and $C_2$ for any integer $m \geq 1$. Hence neither $C_{6m+1}$ nor $C_{6m+2}$ has primitive integral points for any integer $m \geq 1$. We have thus completed the proof.

**Theorem 6.2.** All integer solutions of the Diophantine equation $y^2 = x^3 + 3^n$ are as follows:
The proof is similar to that for Theorem 5.2, so we omit it.

ACKNOWLEDGMENTS

The author would like to express his gratitude to the anonymous referee for many useful and valuable suggestions that improved this paper, in particular the suggestions that the proofs could be made more rigorous, that one could verify that the bounds in Theorems 1.1 and 1.2 are sharp, and that the Diophantine equation $y^2 = x^n + 3^n$ could be resolved.

REFERENCES

[Bilu et al. 01] Y. Bilu, G. Hanrot, and P. Voutier (with an appendix by M. Mignotte). “Existence of Primitive Divisors of Lucas and Lehmer Numbers.” J. Reine Angew. Math. 539 (2001), 75–122.

[Carmichael 13] R. D. Carmichael. “On the Numerical Factors of the Arithmetic Forms $a^n \pm b^n$.” Ann. of Math. 15 (1913), 30–70.

[Cassels 91] J. W. S. Cassels. Lectures on Elliptic Curves. Cambridge: Cambridge University Press, 1991.

[Durst 59] L. K. Durst. “Exceptional Real Lehmer Sequences.” Pacific J. Math. 9 (1959), 437–441.

[Everest et al. 06] G. Everest, G. Mclaren, and T. Ward. “Primitive Divisors of Elliptic Divisibility Sequences.” J. Number Theory 118 (2006), 71–89.

[Ingram 07] P. Ingram. “Elliptic Divisibility Sequences over Certain Curves.” J. Number Theory 123 (2007), 473–486.

[Rabinowitz 77] S. Rabinowitz. “The Solution of $y^2 \pm 2^n = x^3$.” Proc. Amer. Math. Soc. 62 (1977), 1–6.

[Schinzel 74] A. Schinzel. “Primitive Divisors of the Expression $A^n - B^n$ in Algebraic Number Fields.” J. Reine Angew. Math. 268/269 (1974), 27–33.

[Silverman 88] J. H. Silverman. “Wieferich’s Criterion and the ABC-Conjecture.” J. Number Theory 30 (1988), 226–237.

[Silverman and Tate 94] J. H. Silverman and J. Tate. Rational Points on Elliptic Curves. New York: Springer-Verlag, 1994.

[Stewart 77] C. L. Stewart. “Primitive Divisors of Lucas and Lehmer numbers.” In Transcendence Theory: Advances and Applications, edited by A. Baker and D. W. Masser, pp. 79–92. London: Academic Press, 1977.

[Voutier 98] P. M. Voutier. “Primitive Divisors of Lucas and Lehmer Sequences, III.” Math. Proc. Cambridge Phil. Soc. 123 (1998), 407–419.

[Ward 48] M. Ward. “Memoir on Elliptic Divisibility Sequences.” Amer. J. Math. 70 (1948), 31–74.

[Ward 55] M. Ward. “The Intrinsic Divisors of Lehmer Numbers.” Ann. of Math. (2) 62 (1955), 230–236.

[Zsigmondy 92] K. Zsigmondy. “Zur Theorie der Potenzreste.” Monatsh. Math. 3 (1892), 265–284.