ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 39, Number 4, 2009

ELLIPTIC DIVISIBILITY SEQUENCES AND CERTAIN DIOPHANTINE EQUATIONS

MINORU YABUTA

ABSTRACT. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbf{Z}$. For a nontorsion rational point P on E, write $x(nP) = A_n/B_n^2$ in lowest terms. We give a computable constant N such that for all integers $m \geq N$ the term B_{p^m} has a divisor not dividing B_{p^k} for $0 \leq k \leq m-2$. Applying this result to the family of elliptic curves $E_m : y^2 = x^3 + b^{6m+r}$, where E_0 has rank one, we give a computable constant N' such that for all integers $m \geq N'$ the curve E_m has no primitive integral points.

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

$$x(nP) = \frac{A_n(P)}{B_n^2(P)}, \tag{1.1}$$

in lowest terms with $A_n(P) \in \mathbf{Z}$ and $B_n(P) \in \mathbf{N}$. The sequence $\{B_n(P)\}_{n\geq 1}$ is known as an *elliptic divisibility sequence*. It is well known that $B_m(P)|B_n(P)$ whenever $m|n$. Ward [**18**] first studied the arithmetic properties of elliptic divisibility sequences.

For an integer sequence $\{u_n\}_{n\geq 1}$ a prime p is called a *primitive divisor* of u_n if p divides u_n but does not divide u_k for any $0 < k < n$. Silverman [**14**] first showed that for all sufficiently large integers n the term $B_n(P)$ has a primitive divisor. Everest, Mclaren and Ward [**7**] obtained a uniform and quite small bound beyond which a primitive divisor is guaranteed for congruent number curves $y^2 = x^3 - T^2x$ with $T > 0$ square-free. They showed that, if $m > 5$, then $B_{2m}(P)$ has a primitive divisor and that, if $x(P)$ is negative and $m > 2$ or if $x(P)$ is a

2000 AMS *Mathematics subject classification.* Primary 11G05, 11A41, 11D61, 11D45.
Keywords and phrases. Elliptic curve, elliptic divisibility sequence, primitive divisor, diophantine equation, canonical height.
Received by the editors on October 23, 2006, and in revised form on February 1, 2007.
DOI:10.1216/RMJ-2009-39-4-1339

square and $m > 11$, then $B_{2m-1}(P)$ has a primitive divisor. Improving their work, Ingram [**8**] showed that if $x(P) < 0$ and $n > 2$, then $B_n(P)$ has a primitive divisor. Everest and King [**6**] showed that only finitely many terms $B_n(P)$ are prime powers in certain cases.

Now we denote by h the absolute logarithmic height on $\mathbf{Q}$ and by $\hat{h}$ the canonical height on $E(\mathbf{Q})$. In this paper we will give an elementary proof of the following theorem.

Theorem 1.1. *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbf{Z}$ and $c = \max\{|a|, |b|\} \geq 2$. Let $P \in E(\mathbf{Q})$ be a nontorsion point, and let p be a prime. Let N be an integer satisfying*

$$(1.2)\quad 2(p^2-1)p^{2N-4}\hat{h}(P) - \tfrac{5}{12}h(j) - \tfrac{1}{3}h(\Delta) - 4.086 \geq \log\left(p^2(15c)^{p^2/2}\right).$$

Then, for all integers $m \geq N$ the term $B_{p^m}(P)$ has a divisor not dividing $B_{p^k}(P)$ for $0 \leq k \leq m-2$.

Here $\Delta = -16(4a^3 + 27b^2)$ and $j = -1728(4a)^3/\Delta$ are the discriminant of E and the j-invariant of E, respectively. Our methods cannot allow us to state a result like Theorem 1.1 if it has $k < m$. What this paper does is to obtain an explicit bound beyond which the term $B_{p^m}(P)$ has a divisor not dividing $B_{p^k}(P)$ for $0 \leq k \leq m-2$. The case when $p = 2$ is already quite important because the duplication map plays a very important role in the arithmetic of elliptic curves. We anticipate that our results might find applications.

Next, by using Lang's conjecture we obtain a uniform bound independent of $P \in E(\mathbf{Q})$.

Corollary 1.2. *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbf{Z}$ and $c = \max\{|a|, |b|\} \geq 2$. Let $P \in E(\mathbf{Q})$ be a nontorsion point, and let p be a prime. Assume that a or b is zero. If an integer N satisfies*

$$2\kappa(p^2-1)p^{2N-4} > 1/3 + \left(\log\left(p^2(15c)^{p^2/2}\right) + 5.435\right) \Big/ \log|\Delta|,$$

then for all integers $m \geq N$ the term $B_{p^m}(P)$ has a divisor not dividing $B_{p^k}(P)$ for $0 \leq k \leq m-2$, where κ is a uniform positive constant independent of E and P.

Now primitive divisors have been studied by several authors, and there have been many results about primitive divisors. In 1892, Zsigmondy [**19**] 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. Bang [**1**] earlier proved the special case $b = 1$. The sequence $U_n = (\alpha^n - \beta^n)/(\alpha - \beta)$, where $\alpha + \beta$ and $\alpha\beta$ are coprime nonzero integers is called the *Lucas sequence*. In 1913, Carmichael [**3**] showed that if α and β are real, then U_n has a primitive divisor for all $n > 12$. Ward [**17**] and Durst [**5**] extended Carmichael's result to Lehmer sequences. In 1974, Schinzel [**10**] proved that there exists an effectively computable constant n_0 independent of α and β so that U_n has a primitive divisor for all $n > n_0$, when α and β are complex and their quotient is not a root of unity. In 1976, Stewart [**15**] showed that if $n > e^{452}2^{67}$ then U_n has a primitive divisor. In 1998, Voutier [**16**] proved that if $n > 30030$ then the nth term of any Lucas or Lehmer sequence has a primitive divisor. In 2001, Bilu, Hanrot and Voutier [**2**] obtained a major result for Lucas and Lehmer sequences. They proved that if $n > 30$, then the nth term of any Lucas or Lehmer sequence has a primitive divisor.

We next consider the diophantine equation $y^2 = x^3 + b^n$ in the integer variables x, y and n, where b is an integer. 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 $0 \le r < 6$. Applying Theorem 1.1, we will prove the following theorem.

Theorem 1.3. *Let r be a fixed integer with $0 \le r < 6$. Let $E_m : y^2 = x^3 + b^{6m+r}$ be an elliptic curve with $b \in \mathbf{Z}$, and assume that $E : y^2 = x^3 + b^r$ has rank one. Let N be an integer satisfying*

$$2(b^2-1)\big((N-1)\log|b| - \tfrac{1}{12}\log|\Delta| - 0.973\big) \ge \log\big(b^2|15b^r|^{b^2/2}\big) + \tfrac{1}{3}\log|\Delta| + 4.086,$$

where Δ is the discriminant of E. If E_ν has a nontrivial primitive integral point, then E_m has no nontrivial primitive integral points for all integers $m \ge \nu + N$.

This theorem can be restated as saying that for all integers $m \ge \nu + N$ the group $E(\mathbf{Q})$ of rational points on the curve E has no points of the form $(s/b^{2m}, t/b^{3m})$ with $\gcd(s, t) = \gcd(s, b) = \gcd(t, b) = 1$.

Many authors have studied certain diophantine equations of the form $C : y^2 = x^3 + D$, where D is an integer. Many results are assembled in Mordell's book [**9**]. By Siegel's theorem, the set of integral points on the elliptic curve $C : y^2 = x^3 + D$ is finite. By Mordell's theorem, the group of rational points on the curve C is finitely generated. In 1950, Cassels [**4**] gave a complete basis for the group of rational points on the elliptic curve C in the range $|D| \leq 50$. As a special case of Silverman's theorem [**11**], we have that the number of integral points on the elliptic curve C is bounded solely in terms of the rank of the group of rational points. Theorem 1.3 is applied to a smaller class of curves; however, it asserts that the number of primitive integral points is not only bounded but zero.

2. Elliptic division polynomials. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbf{Z}$. We define *division polynomials* ψ_n in $\mathbf{Z}[a, b, x, y]$ for the curve E inductively as follows:

$$\begin{aligned}
&\psi_1 = 1, \quad \psi_2 = 2y,\\
&\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2,\\
&\psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3),\\
&\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 \qquad \text{for } n \geq 2,\\
&2y\psi_{2n} = \psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2) \quad \text{for } n \geq 3.
\end{aligned}$$

We extend these to $\mathbf{Z}$ by defining $\psi_{-n} = \psi_n$ and write $\psi_n(Q)$ for evaluated at the point Q. The following proposition is well known, see Silverman [**13**, page 105].

Proposition 2.1. *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbf{Z}$. Then, for each nontorsion point $Q \in E(\mathbf{Q})$,*

$$x(nQ) = x(Q) - \frac{\psi_{n-1}(Q) \cdot \psi_{n+1}(Q)}{\psi_n(Q)^2}. \tag{2.1}$$

For each nontorsion point $Q = (x, y) \in E(\mathbf{Q})$, we can write

$$\psi_n(Q) = \begin{cases} P_n(x) & \text{for } n \text{ odd} \\ 2yP_n(x) & \text{for } n \text{ even} \end{cases}$$

where $P_n(x) \in \mathbf{Z}[a,b,x]$ satisfies the inductive relations:

$$P_{2n+1} = \begin{cases} P_{n+2}P_n^3 - (2y)^4 P_{n-1}P_{n+1}^3 & \text{for } n \text{ odd} \\ (2y)^4 P_{n+2}P_n^3 - P_{n-1}P_{n+1}^3 & \text{for } n \text{ even,} \end{cases} \tag{2.2}$$

$$P_{2n} = P_n(P_{n+2}P_{n-1}^2 - P_{n-2}P_{n+1}^2). \tag{2.3}$$

Replacing y^2 by $x^3 + ax + b$ gives that

$$P_{2n+1} = \begin{cases} P_{n+2}P_n^3 - 16(x^3+ax+b)^2 P_{n-1}P_{n+1}^3 & \text{for } n \text{ odd} \\ 16(x^3+ax+b)^2 P_{n+2}P_n^3 - P_{n-1}P_{n+1}^3 & \text{for } n \text{ even.} \end{cases} \tag{2.4}$$

For n odd $P_n(x)$ is a polynomial of degree $(n^2-1)/2$ with leading coefficient n, and for n even $P_n(x)$ is a polynomial of degree $(n^2-4)/2$ with leading coefficient $n/2$.

Lemma 2.2. *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbf{Z}$ and $c = \max\{|a|, |b|\} \geq 2$. Then every coefficient of $P_n(x)$ is bounded in absolute value by $(14c)^{(n-1)^2/2}$.*

Proof. We denote by M_n the largest of the absolute values of the coefficients of the polynomial $P_n(x)$, and by p_n the number of terms of $P_n(x)$. Then, for all $n \geq 4$,

$$p_n \leq (n^2+1)/2 \leq (14c)^{(2n-5)/4}. \tag{2.5}$$

We will prove this. For n odd $P_n(x)$ is of degree $(n^2-1)/2$, and for n even $P_n(x)$ is of degree $(n^2-4)/2$, so the estimate $p_n \leq (n^2+1)/2$ holds.

Now, for $0 < k \leq l$, write

$$P_k(x) = \sum_{i=0}^{s} a_i x^i, \quad P_l(x) = \sum_{i=0}^{t} b_i x^i, \quad P_k(x)P_l(x) = \sum_{i=0}^{s+t} c_i x^i.$$

Then, for every coefficient c_r of $P_k(x)P_l(x)$,

$$|c_r| = \left| \sum_{\substack{i+j=r \\ 0 \leq i \leq s \\ 0 \leq j \leq t}} a_i b_j \right| \leq \sum_{\substack{i+j=r \\ 0 \leq i \leq s \\ 0 \leq j \leq t}} |a_i b_j| \leq p_k M_k M_l,$$

where M_k and M_l are the largest of absolute values of coefficients of the polynomials $P_k(x)$ and $P_l(x)$, respectively. Hence, from (2.3) and (2.4) we observe that

$$\begin{aligned} M_{2m} &\le p_{m+1}^3 M_m (M_{m+2} M_{m-1}^2 + M_{m-2} M_{m+1}^2). \\ M_{2m+1} &\le p_m^3 M_{m+2} M_m^3 + 16 \cdot 3^2 p_{m+1}^3 c^2 M_{m-1} M_{m+1}^3 \quad \text{for } m \text{ odd}, \\ M_{2m+1} &\le 16 \cdot 3^2 p_m^3 c^2 M_{m+2} M_m^3 + p_{m+1}^3 M_{m-1} M_{m+1}^3 \quad \text{for } m \text{ even}. \end{aligned}$$

To prove our lemma we use strong induction on n. A direct check gives that the result is true for $n = 1, 2, 3, 4$. We have the estimates $M_3 \le 6c^2$ and $M_4 \le 20c^3$. By using the estimates above, we can show that the result is true for $n = 5, 6, 7, 8$.

Now suppose that the result is true for all $1 \le n \le 2k$ with $k \ge 4$. Then, by using (2.5) and the estimate $1 + 144c^2 \le (14c)^2$, we obtain that

$$\begin{aligned} M_{2k+1} &\le p_{k+1}^3 (1 + 144c^2)(14c)^{2k^2-2k+2} \\ &\le (14c)^{(8k^2-2k+7)/4} \le (14c)^{(2k)^2/2}, \end{aligned}$$

and

$$M_{2k+2} \le 2p_{k+2}^3 (14c)^{2k^2+3} \le 2(14c)^{(8k^2+6k+9)/4} \le (14c)^{(2k+1)^2/2}.$$

Hence, the result is true for $n = 2k+1, 2k+2$. Thus, the result follows by induction. □

Lemma 2.3. *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbf{Z}$ and $c = \max\{|a|, |b|\} \ge 2$. If $|x| > (15c)^{(n-1)^2/2}$, then $P_n(x) > 0$.*

Proof. For $n \ge 3$ we write

$$P_n(x) = \sum_{k=0}^{m} c_k x^k, \quad c_m \ne 0.$$

Put $M = \max\{1, |c_0/c_m|, |c_1/c_m|, \ldots, |c_{m-1}/c_m|\}$. Then, by Lemma 2.2 we have that $M \le (14c)^{(n-1)^2/2}$. Let α be any root of the polynomial $P_n(x)$. If $|\alpha| \le 1$, then obviously $|\alpha| < 1 + M$. If $|\alpha| > 1$, then

$$|\alpha|^m = \left| \sum_{k=0}^{m-1} \frac{c_k}{c_m} \alpha^k \right| \le \sum_{k=0}^{m-1} \left| \frac{c_k}{c_m} \right| |\alpha|^k \le \frac{M(|\alpha|^m - 1)}{|\alpha| - 1} < \frac{M|\alpha|^m}{|\alpha| - 1};$$

therefore, $|\alpha| < 1 + M$. Consequently,

$$|\alpha| < 1 + (14c)^{(n-1)^2/2} < (15c)^{(n-1)^2/2}.$$

Combining with the fact that $P_n(x)$ is of even degree yields our lemma. □

3. Proof of Theorem 1.1. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbf{Z}$. For a nontorsion point $P \in E(\mathbf{Q})$, write $x(nP) = A_n(P)/B_n^2(P)$ in lowest terms with $A_n(P) \in \mathbf{Z}$ and $B_n(P) \in \mathbf{N}$. Let p be a prime. Consider the sequence

$$B_1(P), B_p(P), B_{p^2}(P), \ldots, B_{p^n}(P), \ldots.$$

Definition 3.1. For $P \in E(\mathbf{Q})$, we write $x(P) = A/B$ in lowest terms. We define the *height* of P by $H(P) = \max\{|A|, |B|\}$, the *logarithmic height* of P by $h(P) = \log H(P)$, and the *canonical height* of P by

$$\hat{h}(P) = \lim_{n\to\infty} \frac{h(2^n P)}{4^n}.$$

It is known that $\log B_{p^n}(P)$ is roughly as large as $p^{2n}\hat{h}(P)$, at least when p is odd. Applying the growth rate of $B_{p^n}(P)$, we find that $B_{p^n}(P) > pB_{p^{n-1}}(P)$ for all sufficiently large n, and this leads to the existence of a primitive divisor, see Silverman [**14**]. In this section, we will give a computable constant $N > 0$ such that for all integers $m \geq N$ the term $B_{p^m}(P)$ has a divisor not dividing $B_{p^k}(P)$ for $0 \leq k \leq m-2$.

For a rational number $r \neq 0$, we write $r = p^e u/v$, where p is a prime and u, v are integers prime to p. We define $\mathrm{ord}_p(r)$ by $\mathrm{ord}_p(r) = e$.

For every prime p and every integer $n \geq 1$, we define

$$E_{p^n}(\mathbf{Q}) = \{(x, y) \in E(\mathbf{Q}) : p^{2n} \text{ divides the denominator of } x\}.$$

The following propositions are well known, see [**13**].

Proposition 3.2. *If p is a prime then $E_{p^n}(\mathbf{Q})$ is a subgroup of $E(\mathbf{Q})$.*

Proposition 3.3. *For any point $P \in E_p(\mathbf{Q})$, write $x(nP) = A_n/B_n^2$ in lowest terms. Then, for any prime p,*

$$\mathrm{ord}_p B_n = \mathrm{ord}_p B_1 + \mathrm{ord}_p n.$$

Lemma 3.4. *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbf{Z}$ and $c = \max\{|a|, |b|\} \geq 2$. Let p be a prime, and let $Q \in E(\mathbf{Q})$ be a nontorsion point. Assume that, for $n = N-1, N$,*

$$H(p^n Q) \geq p^2 (15c)^{p^2/2} H(p^{n-1} Q). \tag{3.1}$$

Then the term $B_{p^N}(Q)$ has a divisor not dividing $B_{p^k}(Q)$ for $0 \leq k \leq N-2$.

Proof. For all integers $n \geq 0$, put $Q_n = p^n Q$, and write $x(Q_n) = u_n/v_n^2$ in lowest terms with $v_n > 0$. From Proposition 3.3 we observe that

$$v_{N-1} = \begin{cases} tpv_{N-2} & \text{if } p \mid v_{N-2} \\ t' v_{N-2} & \text{if } p \nmid v_{N-2}, \end{cases}$$

where t and t' are integers prime to v_{N-2}. If v_{N-1} has a divisor not dividing v_{N-2}, then so does v_N. So assume for a contradiction that every prime divisor of v_{N-1} divides v_{N-2}, in other words $t = 1$ or $t' = 1$. If $H(Q_{N-1}) = v_{N-1}^2$, then from (3.1) we have that $v_{N-1} > pv_{N-2}$, which is a contradiction. Hence, $H(Q_{N-1}) = |u_{N-1}|$. Then we have

$$|u_{N-1}| \geq p^2 (15c)^{p^2/2} v_{N-2}^2 \geq (15c)^{p^2/2} v_{N-1}^2,$$

so

$$|x(Q_{N-1})| = \left| \frac{u_{N-1}}{v_{N-1}^2} \right| \geq (15c)^{p^2/2}.$$

Lemma 2.3 implies that

$$P_{p-1}\big(x(Q_{N-1})\big) > 0 \quad \text{and} \quad P_{p+1}\big(x(Q_{N-1})\big) > 0.$$

If $p = 2$, then

$$\psi_{p-1}(Q_{N-1}) \psi_{p+1}(Q_{N-1}) = P_1\big(x(Q_{N-1})\big) P_3\big(x(Q_{N-1})\big) > 0.$$

If $p > 2$, then $p+1$ and $p-1$ are both even, so

$$\psi_{p-1}(Q_{N-1})\psi_{p+1}(Q_{N-1}) = \big(2y(Q_{N-1})\big)^2 P_{p-1}\big(x(Q_{N-1})\big) P_{p+1}\big(x(Q_{N-1})\big) \geq 0.$$

Using (2.1) gives that

$$x(Q_N) = x(Q_{N-1}) - \frac{\psi_{p-1}(Q_{N-1}) \cdot \psi_{p+1}(Q_{N-1})}{\psi_p(Q_{N-1})^2} \leq x(Q_{N-1}).$$

Now for any root α of the polynomial $x^3 + ax + b$, we have $|\alpha| < 1 + c$. So

$$-(1+c) < x(Q_N) \leq x(Q_{N-1}).$$

Furthermore,

$$1 + c < (15c)^{p^2/2} < |x(Q_{N-1})|.$$

Hence, $|x(Q_N)| \leq |x(Q_{N-1})|$. On the other hand, from (3.1) we have $H(Q_N) > p^2 H(Q_{N-1})$. It follows that the term v_N has a divisor not dividing v_{N-1}. Thus, we have completed the proof. □

The following proposition about the height is well known, so the proof may be omitted, see Silverman [**13**, page 229].

Proposition 3.5. *For all $P \in E(\mathbf{Q})$ and $n \in \mathbf{Z}$,*

$$\widehat{h}(nP) = n^2 \widehat{h}(P).$$

Silverman [**12**] gave an explicit estimate for the difference of the logarithmic height and the canonical height of points on elliptic curves in terms of the j-invariant and the discriminant.

Theorem 3.6 [**12**]. *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbf{Z}$. Then, for every $P \in E(\mathbf{Q})$,*

$$\begin{aligned} -\tfrac{1}{8}h(j) - \tfrac{1}{12}h(\Delta) - 0.973 &\leq \widehat{h}(P) - \tfrac{1}{2}h(P) \\ &\leq \tfrac{1}{12}h(j) + \tfrac{1}{12}h(\Delta) + 1.07, \end{aligned} \tag{3.2}$$

where $\Delta = -16(4a^3 + 27b^2)$ *and* $j = -1728(4a)^3/\Delta$ *are the discriminant of* E *and the* j*-invariant of* E*, respectively.*

Now we are ready to prove Theorem 1.1. Set the notations as follows:

$$K_{j,\Delta} = \tfrac{1}{8}h(j) + \tfrac{1}{12}h(\Delta) + 0.973, \tag{3.3}$$

$$L_{j,\Delta} = \tfrac{5}{12}h(j) + \tfrac{1}{3}h(\Delta) + 4.086 \tag{3.4}$$

Proof of Theorem 1.1. From Theorem 3.6 we have that

$$\begin{aligned} h(p^{n+1}P) - h(p^nP) &\geq 2\widehat{h}(p^{n+1}P) - 2\widehat{h}(p^nP) - L_{j,\Delta} \\ &= 2(p^2-1)p^{2n}\widehat{h}(P) - L_{j,\Delta}. \end{aligned}$$

Now

$$2(p^2-1)p^{2N-4}\widehat{h}(P) - L_{j,\Delta} \geq \log\bigl(p^2(15c)^{p^2/2}\bigr);$$

therefore, for all integers $n \geq N-2$,

$$H(p^{n+1}P) \geq p^2(15c)^{p^2/2}H(p^nP).$$

By Lemma 3.4, it follows that for all integers $m \geq N$ the term $B_{p^m}(P)$ has a divisor not dividing $B_{p^k}(P)$ for $0 \leq k \leq m-2$. □

Now Lang's conjecture says that if $P \in E(\mathbf{Q})$ is a nontorsion point then there exists a uniform constant $\kappa > 0$ independent of E and P, so that

$$\widehat{h}(P) \geq \kappa \log \Delta.$$

When a or b is zero, Lang's conjecture is known to be true. If $a = 0$, then $j = 0$ and if $b = 0$, then $j = 1728$. So if a or b is zero, then the condition (1.2) in Theorem 1.1 can be replaced by

$$\begin{aligned} &2(p^2-1)p^{2N-4}\kappa \log \Delta \\ &\qquad > \tfrac{5}{12}\log 1728 + \tfrac{1}{3}\log\Delta + 4.086 + \log\bigl(p^2(15c)^{p^2/2}\bigr). \end{aligned}$$

Canceling all the terms with $\log\Delta$, we have that

$$2\kappa(p^2-1)p^{2N-4} > 1/3 + \Big(\log\big(p^2(15c)^{p^2/2}\big) + 5.435\Big)\Big/ \log\Delta.$$

We have thus completed the proof of Corollary 1.2. □

Corollary 3.7. *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbf{Z}$ and $c = \max\{|a|, |b|\} \geq 2$. Let p be a prime, and assume that $B_1(P) \equiv 0 \mod p$. Let N be an integer satisfying*

$$2(p^2-1)\big((N-1)\log p - K_{j,\Delta}\big) - L_{j,\Delta} \geq \log\big(p^2(15c)^{p^2/2}\big). \tag{3.5}$$

Then, for all integers $m \geq N$, the term $B_{p^m}(P)$ has a divisor not dividing $B_{p^k}(P)$ for $0 \leq k \leq m-2$.

Proof. From Proposition 3.3 we have that $B_{p^n}(P) \equiv 0 \mod p^{n+1}$ for all $n \geq 0$, and therefore

$$h(p^nP) \geq \log B_{p^n}^2(P) \geq 2(n+1)\log p.$$

From Theorem 3.6 we have that, for all $n \geq 0$,

$$\widehat{h}(p^nP) \geq \tfrac{1}{2}h(p^nP) - K_{j,\Delta} \geq (n+1)\log p - K_{j,\Delta}.$$

Hence,

$$p^{2N-4}\widehat{h}(P) = \widehat{h}(p^{N-2}P) \geq (N-1)\log p - K_{j,\Delta}.$$

Using Theorem 1.1 yields our corollary. □

Example 3.8. Let $E : y^2 = x^3 + b$ be an elliptic curve with $b \in \mathbf{Z}$ and $|b| \geq 2$. Then $j = 0$ and $\Delta = -16 \times 27b^2$. Let p be a prime with $p \geq \max\{5, |b|\}$. Then, after a little computation, we obtain that $N = 3$ satisfies (3.5). It follows that if $B_1(P) \equiv 0 \mod p$ then for all integers $m \geq 3$ the term $B_{p^m}(P)$ has a divisor not dividing $B_{p^k}(P)$ for $0 \leq k \leq m-2$.

Our method will guarantee a primitive divisor beyond a certain value, and we can check all smaller values to find when primitive divisors really start to occur.

Example 3.9. The elliptic curve $E : y^2 = x^3 + 3$ has rank one, and $E(\mathbf{Q}) \simeq \langle (1,2) \rangle$. Putting $P = (1,2)$, we have that $2P = (-23/2^4, 11/2^6)$. We substitute $p = 2$ and $c = 3$ into (3.5) and find that $N = 11$ after a little computation. A direct check gives that $B_{2^m}(P)$ has a primitive divisor for all $1 \leq m \leq 11$. It follows that for all $m \geq 2$ the term $B_{2^m}(P)$ has a divisor not dividing $B_{2^k}(P)$ for $0 \leq k \leq m-2$.

4. Proof of Theorem 1.3. Consider the diophantine equation $y^2 = x^3 + b^n$ in the integer variables x, y and n, where b is an integer with $|b| \geq 2$. For the elliptic curve defined by the equation $E : y^2 = x^3 + b$, we define

$$E_b(\mathbf{Q}) = \{(x,y) \in E(\mathbf{Q}) : b^2 \text{ divides the denominator of } x\}.$$

Lemma 4.1. *If the curve $E : y^2 = x^3 + b$ has rank one, then $E_b(\mathbf{Q})$ is an infinite cyclic group.*

Proof. The set $E_b(\mathbf{Q})$ is simply the intersection of $E_{p^e}(\mathbf{Q})$ for all prime powers p^e dividing b. Each $E_{p^e}(\mathbf{Q})$ is torsion free, so $E_b(\mathbf{Q})$ is torsion free. Since $E_b(\mathbf{Q})$ sits inside $\mathbf{Z} \times F$ for a finite group F, it follows that $E_b(\mathbf{Q})$ itself is cyclic. □

We can write $n = 6m + r$ with $0 \leq r < 6$. For a given integer r with $0 \leq r < 6$, assume that the curve defined by the equation $y^2 = x^3 + b^r$ has rank one. Applying Corollary 3.7, we will prove Theorem 1.3.

Proof of Theorem 1.3. If $E_m : y^2 = x^3 + b^{6m+r}$ has a nontrivial primitive integral point (s,t), then $E : y^2 = x^3 + b^r$ has the rational point of the form $(s/b^{2m}, t/b^{3m})$ in lowest terms. This theorem can be restated as saying that for all integers $m \geq \nu + N$ the group $E(\mathbf{Q})$ of rational points on the curve E has no points of the form $(s/b^{2m}, t/b^{3m})$ in lowest terms.

The curve E has rank one, so $E_b(\mathbf{Q})$ is an infinite cyclic group. Let P_0 be a generator for $E_b(\mathbf{Q})$. Write $x(nP_0) = A_n/B_n^2$ in lowest terms. Let k_0 be the least positive value of integers k such that $B_k = b^\nu$. Then,

from Corollary 3.7, we obtain that $B_{b^n k_0}$ has a divisor not dividing b for all integers $n \geq N$. Hence, for any nontorsion point $P \in E(\mathbf{Q})$ if the denominator of $x(P)$ is divided by $b^{2(\nu+N)}$, then it has a divisor not dividing b. It follows that E_m has no nontrivial primitive integral points for all integers $m \geq \nu + N$. □

Example 4.2. Let r and b be fixed integers with $0 \leq r < 6$ and $|b| \geq 12$. Consider the diophantine equation $E_m : y^2 = x^3 + b^{6m+r}$ in the integer variables x, y and m. Assume that the elliptic curve defined by the equation $E : y^2 = x^3 + b^r$ has rank one. If $|b| \geq 12$, then $N = 4$ satisfies that

$$2(b^2-1)\big((N-1)\log|b| - \tfrac{1}{12}\log|\Delta| - 0.98\big) \geq \log\big(b^2|15b^r|^{b^2/2}\big) + \tfrac{1}{3}\log|\Delta| + 4.09,$$

where Δ is the discriminant of E. It follows that if the diophantine equation E_ν has a primitive integral solution, then the equation E_m has no primitive integral solutions for all integers $m \geq \nu + 4$.

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, Corollary 1.2 and Example 3.9 are due to the referee. Moreover, the referee's suggestion that the author should add the more background about primitive divisors strengthened this paper.

REFERENCES

1. A.S. Bang, *Taltheoretiske Undersgelser*, Tidsskrift for Math. **5** (1886), 70–80, 130–137.

2. Yu. 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.

3. R.D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Annals Math. **15** (1913), 30–70.

4. J.W. Cassels, *The rational solutions of the Diophantine equation* $y^2 = x^3 - D$, Acta. Math. **82** (1950), 243–273.

5. L. K. Durst, *Exceptional real Lehmer sequences*, Pacific J. Math. **9** (1959), 437–441.

6. G. Everest and H. King, *Prime powers in elliptic divisibility sequences*, Math. Comp. **74** (2005), 2061–2071.

7. G. Everest, G. Mclaren and T. Ward, *Prime divisors of elliptic divisibility sequences*, J. Number Theory **118** (2006), 71–89.

8. P. Ingram, *Elliptic divisibility sequences over certain curves*, J. Number Theory **123** (2007), 473–486.

9. L.J. Mordell, *Diophantine equations*, Academic Press, London, 1969.

10. A. Schinzel, *Primitive divisors of the expression $A^n - B^n$ in algebraic number fields*, J. reine Angew. Math. **268/269** (1974), 27–33.

11. J.H. Silverman, *A quantitative version of Siegel's theorem: Integral points on elliptic curves and Catalan curves*, J. reine Angew. Math. **378** (1987), 60–100.

12. ———, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. **192** (1990), 723–743.

13. ———, *The arithmetic of elliptic curves*, Graduate Texts Math. **106**, Springer-Verlag, New York, 1986.

14. ———, *Wieferich's criterion and the abc-conjecture*, J. Number Theory **30** (1988), 226–237.

15. C.L. Stewart, *Primitive divisors of Lucas and Lehmer numbers*, Academic Press, London, 1977.

16. P.M. Voutier, *Primitive divisors of Lucas and Lehmer sequences*, Math. Proc. Cambridge Philos. Soc. **123** (1998), 407–419.

17. M. Ward, *The intrinsic divisors of Lehmer numbers*, Annals Math. **62** (1955), 230–236.

18. ———, *Memoir on elliptic divisibility sequences*, Amer. J. Math. **70** (1948), 31–74.

19. K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. **3** (1892), 265–284.

Senri High School, 17-1, 2 chome, Takanodai, Suita, Osaka, 565-0861, Japan
Email address: yabutam@senri.osaka-c.ed.jp