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 $y^2 = x^3 - T^2 x$ 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