Vol. 48, No. 3 DUKE MATHEMATICAL JOURNAL © September 1981

LOWER BOUND FOR THE CANONICAL HEIGHT ON ELLIPTIC CURVES

JOSEPH H. SILVERMAN

1. Introduction. The canonical height on an elliptic curve E defined over a number field K is a function

$$h^* : E(\bar{K}) \to \mathbb{R}.$$

It plays the role on an elliptic curve that the ordinary logarithm plays for number fields, as indicated by the known and conjectural formulas for special values of L-series. Two elementary properties of h^* are the following:

(1) $h^*(P) = 0$ if and only if P is a torsion point.

(2) h^* is a positive definite quadratic form on $E(\bar{K})/\text{torsion}$.

(For basic facts about heights, see [3] or [4].) In view of these, one might be tempted to ask how small $h^*(P)$ can be for non-torsion points P.

CONJECTURE (Serge Lang [3], p. 92): *Let K be a number field. There are constants $c_1, c_2 > 0$, depending only on K, so that for any elliptic curve E/K and any nontorsion point $P \in E(K)$, one has*

$$h^*(P) > c_1 \log|N_{K/\mathbb{Q}} \Delta_{E/K}| + c_2.$$

(Here $\Delta_{E/K}$ is the minimal discriminant of E over K.)

Being unable to settle Lang's conjecture as stated, one might simplify the problem by considering a more restricted class of curves. For example, an immediate corollary of the result of section 4 of this paper will be that Lang's conjecture is true if one takes only elliptic curves with integral j-invariant. As an alternative, one might take all elliptic curves, but only allow a subset of the rational points. This turns out to be a better approach, and we will prove that Lang's conjecture is true for points which are not "too complicated" in a sense to be made precise later.

One reason for studying such lower bounds is their application to the study of integral points on affine models of elliptic curves. For example, if A is a square-free integer, one can prove that the number of integral solutions to $y^2 = x^4 + A$ is bounded by a constant depending only on the rank of this elliptic curve (cf. [2], [3] p. 140, [7]). As explained in [7], one ingredient in the proof is a lower bound for h^*.

From another viewpoint, one might fix an elliptic curve E/K and ask how $h^*(P)$ can vary for nontorsion points $P \in E(\bar{K})$, specifically how $h^*(P)$ varies in terms of the degree of the minimal field of definition of P. Results of this sort are

Received January 28, 1981. Revision received May 18, 1981.