PACIFIC JOURNAL OF MATHEMATICS
Vol. 135, No. 1, 1988

ON A THEOREM DUE TO CASSELS

JOSÉ M. SOUTO MENÉNDEZ

Using properties of one-dimensional formal groups, a proof is given of a theorem on the valuations of the torsion points of elliptic curves defined over p-adic fields.

1. Introduction. The aim of the present note is to give a proof of Theorem 5, due to Cassels, on the valuations of the torsion points of an elliptic curve defined over a local field K of characteristic zero. Cassels's proof relies on the addition formulas for the Weierstrass $\wp$ and $\wp'$ functions. The one given here follows from the properties of the torsion points of one-dimensional formal groups defined over the ring of integers of K.

The reader could also look at Oort [5] for another approach to Cassels' theorem.

2. Torsion points of formal groups. In the following we denote by K a local field, finite extension of the field Q_p of p-adic numbers, with ring of integers A; we assume that the normalized valuation v of K is extended to the algebraic closure $\overline{K}$ of K. We denote by $\mathfrak{p}_K$ (resp. $\mathfrak{p}_{\overline{K}}$) the maximal ideal of A (resp. of the valuation ring of $\overline{K}$), and by $e = v(p)$ the ramification index of K/Q_P.

Let F be a one-dimensional formal group of finite height $h \geq 1$, defined over A; as usual (see [3]), for each $a \in Z_p$ we denote by $[a](X) \in A[[X]]$ the unique endomorphism of F such that $[a](X) = aX + \cdots$. The group of points $F(\mathfrak{p}_{\overline{K}})$ of F with values in $\overline{K}$ has a structure of a module over Z_p, by means of the operation $a \cdot x = [a](x)$, $a \in Z_p$, $x \in F(\mathfrak{p}_{\overline{K}})$; $F(\mathfrak{p}_K)$ is a sub-Z_p-module of $F(\mathfrak{p}_{\overline{K}})$.

Let $[p](X) = \sum_{i=1}^{\infty} a_i X^i$ ($a_1 = p$) be the "multiplication by p" in the formal group F; setting $q = p^h$, one has $a_i \in \mathfrak{p}_K$ if $i = 1, \ldots, q-1$ and $v(a_q) = 0$. We shall be interested in the valuations of the torsion points $x \in F(\mathfrak{p}_{\overline{K}})$. The most convenient thing is to consider the Newton polygon of the series $[p](X)$, that is the lower convex envelope of the points $(i, v(a_i)) \in R^2$ ($i \geq 1$).

If $P_0 = (1, e)$, $P_1 = (q_1, e_1), \ldots, P_m = (q, 0)$ are the vertices of such a polygon (where $e_i = v(a_{q_i})$), the slopes are the negative of the numbers