Vol. 52, No. 1 DUKE MATHEMATICAL JOURNAL © March 1985

THE INVARIANTS OF THE TATE–SHAFAREVICH GROUP IN A $\mathbf{Z}_p$-EXTENSION CAN BE INFINITE

GUDRUN BRATTSTRÖM

It has long been conjectured that the Tate–Shafarevich group of an abelian variety over a number field is finite. The object of this paper is to construct examples showing that the Galois invariants of the p-primary subgroup of the Tate–Shafarevich group over a $\mathbf{Z}_p$-extension can nevertheless be infinite. These examples have the additional property that' the p-adic height pairing is degenerate. The idea for constructing them is first to find a $\mathbf{Z}_p$-extension L_∞ where the p-adic height pairing is degenerate and which is also close p-adically to a $\mathbf{Z}_p$-extension L_∞^0 where the Iwasawa power series attached to a certain Selmer group over L_∞^0 is known explicitly and is not identically zero. One then deduces that the corresponding Iwasawa power series for L_∞ is not identically zero either. It is a consequence of this and the degeneracy of the height paring that the Galois invariants of the Tate–Shafarevich group over L_∞ are infinite. (See Proposition 3.)

By a theorem of Perrin-Riou ([9] and [10]) and Schneider ([12] and [13]), the p-adic height pairing is degenerate if and only if the above-mentioned Iwasawa power series has a zero at $T = 0$ of order strictly greater than the rank of the curve. Since this power series is related to the two-variable p-adic L-function via the two-variable Main Conjecture (see [5] and [14]), this suggests that a p-adic Birch and Swinnerton-Dyer conjecture would have to be more subtle than its complex counterpart. Moreover, in the situation described above the power series is not identically zero, so in particular it has a leading coefficient. It is however difficult to imagine an arithmetic interpretation for this coefficient.

I wish to thank John Coates, Catherine Goldstein and Bernadette Perrin-Riou for numerous and illuminating conversations on the topics discussed in this paper. I also thank Barry Mazur, who made several valuable suggestions.

§1. Iwasawa modules attached to Selmer groups. Let E be an elliptic curve defined over $\mathbf{Q}$ with complex multiplication by the full ring of integers $\mathfrak{o}$ in an imaginary quadratic field K (which therefore will have class number one). We choose the isomorphism $i : \mathrm{End}(E) \to \mathfrak{o}$ such that $\eta^*\omega = i(\eta)\omega$ for all differentials ω of the first kind defined over $\mathbf{Q}$ and all $\eta \in \mathrm{End}(E)$. Let p be a rational prime which is not equal to 2 or 3, and where E has good ordinary reduction. In

Received Feb. 20, 1984. Revision received July 13, 1984.