JONATHAN LUBIN

Canonicity of a cyclic subgroup of an elliptic curve

Astérisque, tome 63 (1979), p. 165-167
<http://www.numdam.org/item?id=AST_1979__63__165_0>

Société Mathématique de France
Astérisque 63 (1979) p. 165-168

CANONICITY OF A CYCLIC SUBGROUP OF AN ELLIPTIC CURVE

Jonathan LUBIN
(Providence)

The story begins with an observation made by Mazur in [1]. Let p be a prime, and suppose an elliptic curve E defined over a number field K has E_p (the groupscheme kernel of multiplication by p) isomorphic to $\boldsymbol{\mu}_p \oplus \mathbf{Z}/p\mathbf{Z}$. Then for all finite extension fields L of K , the $\mathbf{F}(p)$-dimension of the Selmer group $\mathcal{S}^{(p)}(E,L)$ is at least $[L:\mathbf{Q}]/2 - c$, for a fixed c . This is Proposition 10.1 of [1], and it follows from the fact that $\mathcal{S}^{(p)}$ is essentially an H^1 with coefficients in E_p , except for primes where the reduction is unseemly (malséante), and from the fact that $H^1(\boldsymbol{\mu}_p)$ is U_L/U_L^p , where U_L is the group of global units of L . My aim has been to find cases where the rank of the Selmer group might increase at least linearly with $[L:\mathbf{Q}]$, other than the very special case mentioned by Mazur, whose hypothesis on E_p means not merely that E is ordinary at every prime $\mathfrak{P}$ of K dividing p , but that the cyclic subgroup of $E_p(\overline{K})$ that is annihilated by reduction modulo $\mathfrak{P}$ is the same for all such $\mathfrak{P}$.

The results given below are stated for elliptic curves with integral j-invariant, but the modifications necessary for the general case are all easily made. Having made this assumption on j , we may pass to a finite extension of K over which E everywhere has reduction that is seemly (bienséante), and so may ignore unseemly reduction of additive type.

This research was supported by a grant from the National Science Foundation.

The Selmer group fits into the exact sequence

$$0 \longrightarrow E(K)/pE(K) \longrightarrow \mathfrak{S}^{(p)}(E,K) \longrightarrow Ш(E,K)_p \longrightarrow 0 \quad ,$$

and it is computed from purely local data. If E is ordinary at a prime $\mathfrak{P}$ dividing p, the only important datum to know is which one of the $p+1$ proper subgroups of $E_p(\bar{K})$ is canonical in the sense that its elements are annihilated by reduction modulo $\mathfrak{P}$. In the supersingular case, all points of E_p are annihilated by reduction modulo $\mathfrak{P}$, but it may be that p of them form a canonical subgroup in the sense that they are $\mathfrak{P}$-adically closer to the identity than the other p^2-p points of $E_p(\bar{K})$. This happens exactly when the Hasse invariant h of E, computed in the well-known way not modulo $\mathfrak{P}$ but modulo p, satisfies the condition $v_{\mathfrak{P}}(h) < p/(p+1)$, where $v_{\mathfrak{P}}$ is the $\mathfrak{P}$-adic valuation, normalized so that $v_{\mathfrak{P}}(p)=1$. In either the ordinary or supersingular case, then, if S is a subgroup of $E(\bar{K})$ of order p, we will say that the local canonicity of S is zero, $c_{\mathfrak{P}}(S)=0$, if S is not canonical at $\mathfrak{P}$; and $c_{\mathfrak{P}}(S)=1-\frac{p+1}{p}v_{\mathfrak{P}}(h)$ if S is canonical at $\mathfrak{P}$. The global canonicity of S is the weighted sum of the local canonicities:

$$c(S) = \sum_{\mathfrak{P}|p} \frac{n_{\mathfrak{P}}}{n} c_{\mathfrak{P}}(S) \qquad ,$$

where $n_{\mathfrak{P}}$ is the local degree $[K_{\mathfrak{P}}:\mathbf{Q}_p]$ and n is the global degree $[K:\mathbf{Q}]$. Canonicity is clearly invariant under extension of the base field, and $c(S)=1$ is just the case that Mazur mentioned.

The computation necessary to connect the canonicity with the local contributions to the Selmer group was first done by L. Roberts (in [3], and quoted as Proposition 9.3 of [2]). With this, we can prove:

Theorem 1. _Let_ E _be an elliptic curve defined over the number field_ K_0, _with j-invariant integral, and let_ S _be a subgroup of_ $E(\overline{K_0})$ _of order_ p. _Then there is a finite extension_ K _of_ K_0, _such that for every field_ L _finite over_ K,

$$\dim_{\mathbf{F}(p)} \mathfrak{S}^{(p)}(E,L) \geq (c(S) - \tfrac{1}{2})[L:\mathbf{Q}] \ .$$

(The field K need only be large enough for E over K to have seemly reduction everywhere, for $E_p(K)$ to equal $E_p(\overline{K})$, and for K to be totally complex.)

The way that the Hasse invariant behaves under isogeny of degree p enables us to prove also:

Theorem 2. <u>Let</u> E_0 <u>be an elliptic curve defined over a number field</u> K_0, <u>with j-invariant integral, and let</u> $\varepsilon > 0$ <u>and the prime number</u> p <u>be given. Then there exist: a finite extension-field</u> K <u>of</u> K_0; <u>an elliptic curve</u> E <u>defined over</u> K <u>and</u> K<u>-isogenous to</u> E_0; <u>and a subgroup</u> S <u>of</u> $E(K)$ <u>of order</u> p, <u>such that</u>

$$c(S) > 1 - \varepsilon .$$

For such a curve,

$$\dim_{\mathbf{F}(p)} \mathcal{S}^{(p)}(E,L) > (\tfrac{1}{2} - \varepsilon)[L:\mathbf{Q}] .$$

References:

[1] B. Mazur, Rational points of Abelian varieties with values in towers of number fields, Invent. Math. <u>18</u> (1972), p. 183-266.

[2] ——— and L. Roberts, Local Euler characteristics, Invent. Math. <u>9</u> (1970), p. 201-234.

[3] L. Roberts, On the flat cohomology of finite groups, Harvard thesis, 1968.

Jonathan LUBIN
Mathematics Department
Brown University
Providence, Rhode Island 02912
U.S.A.