Symbol Length in Brauer Groups of Elliptic Curves

Mateo Attanasio[1], Caroline Choi[1], Andrei Mandelshtam[1], Charlotte Ure[2]

[1]Stanford University [2]University of Virginia

Main Results

Let ℓ be an odd prime integer, and let K be a field of characteristic not $2, 3$ and coprime to ℓ containing a primitive ℓ-th root of unity. For an elliptic curve E over K, we consider the standard Galois representation

$$\rho_{E,\ell} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{F}_\ell),$$

and denote the fixed field of its kernel by L. The Brauer group $\mathrm{Br}(E)$ of an elliptic curve E is an important invariant. A theorem by Merkurjev and Suslin implies that every element of the ℓ-torsion ${}_\ell\mathrm{Br}(E)$ can be written as a product of symbol algebras. Recently, the last author gave an algorithm to compute elements in the Brauer group explicitly, deducing an upper bound of the symbol length in ${}_\ell\mathrm{Br}(E)/{}_\ell\mathrm{Br}(K)$ of $\frac{2}{\ell}[L:K]$ if ℓ divides $[L:K]$ and $2[L:K]$ otherwise. Since $[L:K]$ divides the order of $\mathrm{SL}_2(\mathbb{F}_\ell)$, this implies that the symbol length is always bounded above by $2(\ell+1)(\ell-1)$. Combining this with an algorithm by Rosset-Tate for corestrictions and explicit norm computations, we improve this bound to $[L:K]-1$ in the case that $\ell \nmid [L:K]$. Under the additional assumption that $\mathrm{Gal}(L/K)$ contains an element of order $d > 1$, the symbol length of ${}_\ell\mathrm{Br}(E)/{}_\ell\mathrm{Br}(K)$ is bounded above by $(1-\frac{1}{d})[L:K]$. In particular, these bounds hold for all CM elliptic curves, in which case we deduce an upper bound of $\ell+1$ on the symbol length. We provide an algorithm implemented in SageMath to compute these symbols explicitly over number fields.

Basic Definitions

A **central simple algebra** (CSA) over F is a finite F-algebra with centre F and no non-trivial two-sided ideals. The **Brauer group** $\mathrm{Br}(F)$ of a field F with absolute Galois group G_F is $H^2(G_F, (F^{sep})^\times)$. It may be identified with equivalence classes of central simple algebras over F under the operation of tensor product, where $A \sim B$ if and only if there exist m, n such that we have an isomorphism of matrix algebras $M_n(A) \cong M_m(B)$.

A **symbol algebra** over a field F containing a primitive ℓ-th root of unity is a CSA of the form

$$(a,b)_{\ell,F} := F\left\langle x, y : x^\ell = a, y^\ell = b, xy = \zeta_\ell yx \right\rangle$$

For Brauer groups $\mathrm{Br}(F)$, the **symbol length** $\mathrm{len}_F(n)$ is minimal such that every Brauer class of order dividing n has a representative equal to a tensor product of $\mathrm{len}_F(n)$ symbol algebras. We wish to upper bound the symbol length, which exists by the following theorem:

Theorem 1: A theorem of Merkurjev and Suslin

Let F be a field with a primitive ℓ-th root of unity. Then every element of the ℓ-torsion of the Brauer group, written as ${}_\ell\mathrm{Br}(F)$, can be expressed as a tensor product of symbol algebras.

An explicit computation of the Brauer group of an Elliptic Curve

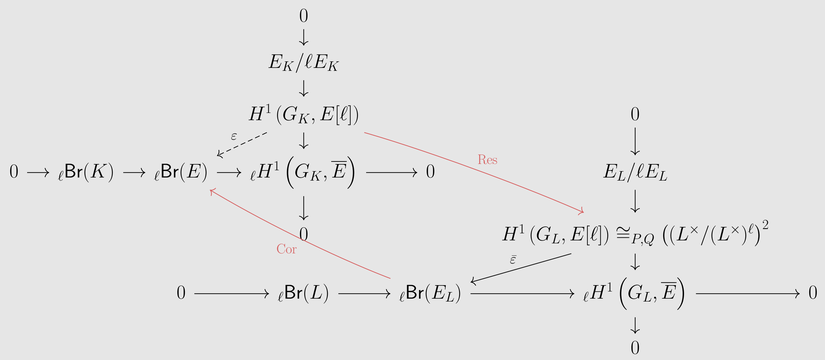
We focused our attention on the special case of elliptic curves: the Brauer group $\mathrm{Br}(E)$ of an elliptic curve E defined over a field K is a torsion abelian group and a subgroup of the Brauer group of its function field $\mathrm{Br}(K(E))$. It is also isomorphic to the unramified Brauer group of $K(E)$ by purity. We seek to understand the prime torsion of $\mathrm{Br}(E)$ through the exact sequence

$$0 \longrightarrow {}_\ell\mathrm{Br}(K) \xrightarrow{i} {}_\ell\mathrm{Br}(E) \xrightarrow{r} {}_\ell H^1(G_K, \overline{E}) \longrightarrow 0\ .$$

We will now describe a split to r that gives us the desired decomposition of ${}_\ell\mathrm{Br}(E)$. We will use a map $\varepsilon : H^1(G_K, E[\ell]) \to {}_\ell\mathrm{Br}(E)$. For reasons given by Chernousov and Guletskiĭ 2001 and Ure 2019, this will induce a split to r, allowing us to write ${}_\ell\mathrm{Br}(E) = {}_\ell\mathrm{Br}(K) \oplus \mathrm{Im}(\varepsilon)$. When all ℓ-torsion points are rational, we can define our map ε as follows. First, fix a basis P, Q for the torsion group $E[\ell]$, which gives us an isomorphism $E[\ell] \xrightarrow{\sim} \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. Then there is an isomorphism from $H^1(K, E[\ell])$ to $\left((K^\times/(K^\times)^\ell\right)^2$ by Kummer theory. The map ε is given by

$$(a,b) \mapsto (a, t_P)_{\ell,K(E)} \otimes (b, t_Q)_{\ell,K(E)}.$$

In the more general case we take L to be the minimal extension of K such that the ℓ-torsion is rational. If $\ell \nmid [L:K]$, then restriction is injective and corestriction is surjective, we define $\bar{\varepsilon}$ as before and use the following diagram to define ε as the composition $[L:K] \circ \varepsilon = \mathrm{Cor} \circ \bar{\varepsilon} \circ \mathrm{Res}$:



Techniques for computing Restriction and Corestriction

We can calculate the image of the restriction map by exploiting the fact that $\mathrm{Res} \circ \mathrm{Cor}$ is a norm map and that Cor is surjective.
On the level of symbol algebras, this acts by choosing a basis P, Q of $E[\ell]$. Then by Kummer theory

$$H^1(G_L, E[\ell]) \cong_{P,Q} H^1(G_L, \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}) \cong H^1(G_L, \mathbb{Z}/\ell\mathbb{Z}) \times H^1(G_L, \mathbb{Z}/\ell\mathbb{Z}) \cong L^\times/(L^\times)^\ell \times L^\times/(L^\times)^\ell$$

Writing $g^{-1} = \begin{pmatrix} c_1^g & c_3^g \\ c_2^g & c_4^g \end{pmatrix}$, this action is given explicitly by

$$g \cdot (a,b) = \left(\left(g^{-1}(a)\right)^{c_1^g} \left(g^{-1}(b)\right)^{c_3^g}, \left(g^{-1}(a)\right)^{c_2^g} \left(g^{-1}(b)\right)^{c_4^g} \right).$$

To compute corestriction, we use an algorithm given in Rosset and Tate 1983, p. 44, which we implemented in SageMath. The definition of the algorithm tells us immediately that the corestriction of a single symbol algebra can be written as the product of $[L:K]$ symbol algebras: this gives a bound of $2[L:K]$ on the symbol length. Exploiting the fact that we only computed corestriction on elements of the image of the norm map allowed us to significantly improve this bound.

Theorem 2: New bounds

If there exists an element of the Galois group σ of order $d > 2$, we can pick a basis such that $\sigma(P) = Q$, and such that all elements of the norm map are of the form

$$(a, t_P)_{\ell,L(E)} \otimes (\sigma(a^{-1}, t_{\sigma(P)})_{\ell,L(E)}$$

Since corestriction is invariant under the Galois action, we see that this has the same corestriction as

$$\mathrm{Cor}\left(\alpha, \frac{t_P}{\sigma^2(t_P)}\right)_{\ell,L(E)}$$

Furthermore we know that α has norm 1: this tells us that the first step in Rosset & Tate's algorithm gives us a trivial symbol algebra. Together, these give us an upper bound on the symbol length of $[L:K]-1$, as long as $[L:K] > 2$ and $\ell \nmid [L:K]$.
Furthermore, if the Galois group of L/K has a subgroup of order $d > 1$, then we pick an intermediate subfield K', apply the above result to the extension L/K', then apply corestriction again from K' to K. This gives an upper bound of $(1-\frac{1}{d})[L:K]$.

Theorem 3: CM Elliptic Curves

The hypotheses hold in the case of CM elliptic curves over number fields. In this case we can exploit knowledge of the admissible subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$. We know that the image of the Galois representation is either contained in a split or a nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. In the first case we have an upper bound on the symbol length of $\ell-1$, and in the latter case we have a bound of $\ell+1$.

Acknowledgements

This research was done as part of the 2021 Number Theory REU at the University of Virginia. We would like to thank everybody involved with organizing, lecturing, and mentoring at the REU. In particular, we would like to thank Ken Ono for managing the REU and his advice and valuable comments on this project. We thank Andrew Sutherland and Wei-Lun Tsai for their assistance on SageMath code. We are grateful for the generous support of the National Science Foundation (Grants DMS 2002265 and DMS 205118), the National Security Agency (Grant H98230-21-1-0059), the Thomas Jefferson Fund at the University of Virginia, and the Templeton World Charity Foundation.

References

Ure, C. (2019). *Prime Torsion in the Brauer Group of an Elliptic Curve*. arXiv: 1909.05317 [math.AG].

Chernousov, V. and V. Guletskiĭ (2001). "2-torsion of the Brauer group of an elliptic curve: generators and relations". In: *Proceedings of the Conference on Quadratic Forms and Related Topics (Baton Rouge, LA, 2001)*. Extra Vol. Pp. 85–120.

Rosset, S. and J. Tate (1983). "A reciprocity law for K_2-traces". In: *Comment. Math. Helv.* 58.1, pp. 38–47. ISSN: 0010-2571. DOI: 10.1007/BF02564623. URL: https://doi.org/10.1007/BF02564623.