Received: 16 September 2022 | Revised: 8 April 2024 | Accepted: 10 April 2024

DOI: 10.1112/blms.13094

RESEARCH ARTICLE

Bulletin of the London Mathematical Society

p^∞-Selmer ranks of CM abelian varieties

Jamie Bell

Department of Mathematics, University College London, London, UK

Correspondence
Jamie Bell, Department of Mathematics, University College London, Gower St, London WC1E 6BT, UK.
Email: james.bell.20@ucl.ac.uk

Funding information
Engineering and Physical Sciences Research Council, Grant/Award Number: EP/S021590/1

Abstract

For an elliptic curve with complex multiplication over a number field, the p^∞-Selmer rank is even for all p. Česnavičius proved this using the fact that E admits a p-isogeny whenever p splits in the complex multiplication field, and invoking known cases of the p-parity conjecture. We give a direct proof, and generalise the result to abelian varieties.

MSC 2020
11G15 (primary), 14K22 (secondary)

1 | INTRODUCTION

An elliptic curve over a number field with endomorphisms other than multiplication by an integer is said to have complex multiplication. These can make the curves easier to work with. It is well-known, and important for this paper, that they always have even rank. Indeed, suppose we have an elliptic curve E over K with complex multiplication, and note that $E(K) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a vector space over $\mathbb{Q}$ with dimension equal to the rank of E. Now the endomorphisms must in fact form a lattice in an imaginary quadratic field L. Then $E(K) \otimes_{\mathbb{Z}} \mathbb{Q}$ is an L-vector space, and so an even-dimensional $\mathbb{Q}$-vector space.

It is not hard to prove that these curves also have root number 1 [1, Proposition 6.3], so they satisfy the parity conjecture. We might hope that there is an analogous result for Selmer groups, that is, that the p^∞-Selmer ranks (defined below) are even, and hence the curves satisfy the p-parity conjecture. This is in fact true, however it is not so easy to prove. In this paper we will present a new proof of this result, and generalise it to abelian varieties (Theorem 1). One might hope that a proof analogous to that for ranks works, as this is also a question of finding the rank of a vector space on which L acts. To see why this proof fails, note that we are now looking at $\mathbb{Q}_p$-vector spaces. The argument for ranks used the fact that a $\mathbb{Q}$-vector space acted on by L has even $\mathbb{Q}$-rank, but this is not true when we replace $\mathbb{Q}$ by $\mathbb{Q}_p$. For example, suppose $p = 5$ and $L = \mathbb{Q}(i)$. Then we can have an action of L on a one-dimensional $\mathbb{Q}_p$-vector space, because $i \in \mathbb{Q}_5$. The method works when p is inert in L, but not when it splits.

Suppose we have an elliptic curve E over a number field K, which has complex multiplication. Looking at the Tate–Shafarevich group Ш, we find its p-primary part is isomorphic to (finite group) $\times (\mathbb{Q}_p/\mathbb{Z}_p)^{\delta_p}$ for some integer δ_p. We will define the p^∞-Selmer rank to be $\mathrm{rk}_p(E) = \mathrm{rk}(E) + \delta_p$.

A generalisation of elliptic curves is abelian varieties. The aim of this paper is to prove the following:

Theorem 1. *Suppose A/K is an abelian variety with complex multiplication by a field M (see Definition 4), and p a prime. Then $\mathrm{rk}_p(A)$ is even.*

Given that the rank is even, Theorem 1 is equivalent to the statement that the divisible part of Ш has even $\mathbb{Z}_p$-corank. This is in fact expected to be 0, as Ш is conjectured to be finite.

Another reason to expect Theorem 1 to hold is the p-parity conjecture, which states that for an abelian variety A over a number field K, with root number $w(A/K)$,

$$(-1)^{\mathrm{rk}_p(A/K)} = w(A/K).$$

In the CM case, the root number is 1 [9, Remark 2 after Theorem 4], so Theorem 1 is equivalent to the p-parity conjecture for abelian varieties with complex multiplication. In a different form p-parity was conjectured by Selmer in 1954 [8]. The conjecture is known in the case where A is an elliptic curve over a number field admitting a p-isogeny thanks to T. Dokchitser and V. Dokchitser [4] and Česnavičius [1]. By calculating root numbers, this allowed Česnavičius to conclude that for elliptic curves with complex multiplication, $\mathrm{rk}_p(A)$ is even. However, there is no equivalent p-parity result to use for abelian varieties, so we must use a different method.

Throughout the paper, we use 'complex multiplication' or 'CM' to mean complex multiplication defined over K. With CM defined over $\bar{\mathbb{Q}}$, the p-parity conjecture has been proved for elliptic curves over totally real K, but is open in general. For $p \neq 2$ this is due to Nekovar [7, 5.10] and for $p = 2$ Green and Maistret [5, 6.5].

From Theorem 1, we can deduce the following:

Corollary 2. *Suppose A and p are as in Theorem 1. If Ш$[p^\infty]$ is infinite, then it contains $(\mathbb{Q}_p/\mathbb{Z}_p)^2$.*

Notation

Throughout, we will assume A and B are abelian varieties over a number field K.

We will denote the dual of an abelian variety A by $\hat{A}$, and of an isogeny $f : A \to B$ by $\hat{f} : \hat{B} \to \hat{A}$.

Let $\lambda : A \to \hat{A}$ be some polarisation of A defined over K.

For an isogeny f and a field L, denote by $f_{A(L)}$ the map on L-points induced by f, and similarly let $f_{Ш}$ be the map induced on the Tate–Shafarevich group.

For a prime p, Ш$[p^\infty]$ is the p-primary part of Ш. δ_p will denote the multiplicity of $\mathbb{Q}_p/\mathbb{Z}_p$ in Ш$[p^\infty]$. Specifically, Ш$[p^\infty] \cong$ (finite group) $\times (\mathbb{Q}_p/\mathbb{Z}_p)^{\delta_p}$ for some integer δ_p. Ш$_d$ will be the divisible part of Ш and Ш$_{nd}$ the quotient of Ш by Ш$_d$.

Write $Y_p(A/K)$ for $\mathrm{Hom}(Ш_d[p^\infty], \mathbb{Q}_p/\mathbb{Z}_p)$, the Pontryagin dual of Ш$_d[p^\infty]$. Let $\mathcal{Y}_p(A/K) = Y_p(A/K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Note this is a $\mathbb{Q}_p$-vector space of dimension δ_p, and an $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}_p$-module.

Definition 3 (Rosati involution). For an abelian variety A with polarisation λ, the Rosati involution is the involution on $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ sending f to $f^\dagger := \lambda^{-1} \circ \hat{f} \circ \lambda$. We extend this by continuity to $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}_p$.

Definition 4 (Complex multiplication). We say A has complex multiplication if

- $\mathrm{End}_K(A) \otimes \mathbb{Q} \supset M$, where M is a totally complex field containing a totally real field L, $[M : L] = 2$ and $[L : \mathbb{Q}] = \dim(A)$;
- the Rosati involution corresponds to complex conjugation on M.

Note that this is complex multiplication over K, not over $\bar{K}$ (which is sometimes called potential complex multiplication).

2 | SELF-ISOGENIES

Suppose A and B are abelian varieties over a number field K, and $f : A \to B$ an isogeny between them.

Recall the following theorem.

Theorem 5 [6, Proof of I.7.3, I.7.3.1]. *There is some finite set S of places of K such that*

$$\prod_{v \in S} \frac{\#\ker(f_{A(K_v)})}{\#\mathrm{coker}(f_{A(K_v)})} = \frac{\#\ker(f_{A(K)})}{\#\mathrm{coker}(f_{A(K)})} \cdot \frac{\#\mathrm{coker}(\hat{f}_{\hat{B}(K)})}{\#\ker(\hat{f}_{\hat{B}(K)})} \cdot \frac{\#\ker(\hat{f}_{\text{Ш}})}{\#\ker(f_{\text{Ш}})}.$$

Corollary 6. *Suppose that $A = B$, that is, f is a self-isogeny. Then*

$$\#\ker(\hat{f}_{\text{Ш}}) = \#\ker(f_{\text{Ш}}).$$

Proof. In the formula in Theorem 5, the left-hand side is equal to the ratio of the volume forms of A and B that appear in the formula for $\frac{L^{(r)}(A,1)}{r!}$ predicted by the Birch–Swinnerton-Dyer conjecture (see [6, Section I.7] for a full definition; in the notation of this chapter the volume term is $\frac{\prod_{v\in S}\mu_v(A,\omega)}{|\mu|^d}$). These depend only on A and not f so when $A = B$, this is 1.

Similarly, the next two terms equal the ratio of the regulators of A and B and the orders of their torsion subgroups. Specifically,

$$\frac{\#\ker(f_{A(K)})}{\#\mathrm{coker}(f_{A(K)})} \cdot \frac{\#\mathrm{coker}(\hat{f}_{\hat{B}(K)})}{\#\ker(\hat{f}_{\hat{B}(K)})} = \frac{\mathrm{Reg}(A/K)\#B(K)_{tors}\#\hat{B}(K)_{tors}}{\mathrm{Reg}(B/K)\#A(K)_{tors}\#\hat{A}(K)_{tors}},$$

therefore when $A = B$ this is also 1. □

The following variant of this result will be useful.

Lemma 7. *Suppose f is as above, and p any prime. Then*

$$\#\ker(\hat{f}_{\text{Ш}[p^\infty]}) = \#\ker(f_{\text{Ш}[p^\infty]}),$$

Proof. For any prime p, the p-adic valuations of the kernels in Lemma 6 must be equal. As both kernels decompose as a product over primes l of their l-primary subgroups, the p-part of each side comes from $Ш[p^\infty]$, so we can replace Ш by $Ш[p^\infty]$ and still have equality. □

Lemma 8. *Suppose f is as before. Then we can split the kernels into divisible and non-divisible parts. Specifically,*

$$\#\ker(\hat{f}_{Ш_d})\#\ker(\hat{f}_{Ш_{nd}}) = \#\ker(f_{Ш_d})\#\ker(f_{Ш_{nd}}).$$

Proof. We will show $\#\ker(f_Ш) = \#\ker(f_{Ш_d})\#\ker(f_{Ш_{nd}})$ and similarly for $\hat{f}$. This holds by an application of the snake lemma to the exact sequence

$$0 \to Ш_d \to Ш \to Ш_{nd} \to 0$$

with the isogeny f, which is valid because f maps $Ш_d$ to $Ш_d$. We can also see that $\#\text{coker}(f_{Ш_d}) = 1$, because f has a conjugate isogeny $g : A \to A$. This has the property that $f \circ g = [\deg(f)]$, and multiplication by an integer is surjective on $Ш_d$. The result follows. □

Lemma 9. *Let A/K be an abelian variety, p a prime, and $f : A \to A$ an isogeny defined over K. Then*

$$\#\ker(\hat{f}_{Ш_d[p^\infty]}) = \#\ker(f_{Ш_d[p^\infty]}).$$

Proof. By the functoriality and non-degeneracy of the Cassels–Tate pairing on $Ш_{nd}$,

$$\#\ker(\hat{f}_{Ш_{nd}[p^\infty]}) = \#\text{coker}(f_{Ш_{nd}[p^\infty]})$$

[6, proof of I.7.3]. Now $\#\text{coker}(f_{Ш_{nd}[p^\infty]})$ and $\#\ker(f_{Ш_{nd}[p^\infty]})$ are equal, because $Ш_{nd}[p^\infty]$ is a finite group. So, the non-divisible parts of the equation in Lemma 8 cancel out, and we have equality of the divisible parts. □

3 | COMPLEX MULTIPLICATION

Recall $Y_p(A/K) := \text{Hom}(Ш_d[p^\infty], \mathbb{Q}_p/\mathbb{Z}_p)$ and $\mathcal{Y}_p(A/K) := Y_p(A/K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Note this is an $\text{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}_p$-module. For ϕ a self-isogeny of A, denote the map induced on $Y_p(A/K)$ by ϕ_{Y_p}, and similarly if $\phi \in \text{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}_p$, denote the map induced on $\mathcal{Y}_p(A/K)$ by $\phi_{\mathcal{Y}_p}$.

Lemma 10. *Suppose A/K is a polarised abelian variety, p a prime, and ϕ an invertible element of* $\text{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}_p$. *Then*

$$\text{ord}_p \det(\phi_{\mathcal{Y}_p}) = \text{ord}_p \det(\phi^\dagger_{\mathcal{Y}_p}).$$

Proof. We prove this for ϕ an isogeny of A defined over K, and the full result follows. By properties of Pontryagin duality,

$$\#\ker(\phi_{Ш_d[p^\infty]}) = \#\text{coker}(\phi_{Y_p}).$$

Now ϕ_{Y_p} can be represented over $\mathbb{Z}_p$ by a matrix P in Smith normal form, with all diagonal entries non-zero. Then

$$\mathrm{ord}_p\det(\phi_{\mathcal{Y}_p}) = \mathrm{ord}_p\det(P) = \mathrm{ord}_p\#\mathrm{coker}(\phi_{Y_p}).$$

It therefore follows from Lemma 9 that

$$\mathrm{ord}_p\det(\phi_{\mathcal{Y}_p}) = \mathrm{ord}_p\det(\hat{\phi}_{\mathcal{Y}_p}).$$

Now as $\hat{\phi} = \lambda\circ\phi^\dagger\circ\lambda^{-1}$, $\phi^\dagger_{\mathcal{Y}_p}$ will have the same determinant, and the result follows. □

Suppose from now on that A has complex multiplication by a field M, with totally real subfield L. Now $\mathcal{Y}_p(A/K)$ is an $M\otimes_{\mathbb{Q}}\mathbb{Q}_p$-module. $M\otimes_{\mathbb{Q}}\mathbb{Q}_p$ is isomorphic to $\prod_{\mathfrak{p}|p} M_{\mathfrak{p}}$, where the product is over primes $\mathfrak{p}$ of M lying above p, and $M_{\mathfrak{p}}$ is the completion of M at $\mathfrak{p}$. We can therefore decompose $\mathcal{Y}_p(A/K)$ into a sum of $\mathbb{Q}_p$-vector spaces

$$\mathcal{Y}_p(A/K) = \bigoplus_{\mathfrak{p}|p} V_{\mathfrak{p}},$$

where each $V_{\mathfrak{p}}$ is an $M_{\mathfrak{p}}$-vector space.

Lemma 11. *For each prime $\mathfrak{p}|p$, we have*

$$\dim_{\mathbb{Q}_p} V_{\mathfrak{p}} = \dim_{\mathbb{Q}_p} V_{\bar{\mathfrak{p}}}.$$

Proof. If $\mathfrak{p} = \bar{\mathfrak{p}}$, we are done, so suppose they are not equal. Then define α to be the element of $M\otimes_{\mathbb{Q}}\mathbb{Q}_p = \prod_{\mathfrak{p}|p} M_{\mathfrak{p}}$ that corresponds to p in $M_{\mathfrak{p}}$ and 1 in all the other factors. Now we can view α as an element of $\mathrm{End}_K(A)\otimes_{\mathbb{Z}}\mathbb{Q}_p$. Then

$$\mathrm{ord}_p\det(\alpha_{\mathcal{Y}_p(A/K)}) = \mathrm{ord}_p\det(p|V_{\mathfrak{p}}) = \dim_{\mathbb{Q}_p} V_{\mathfrak{p}}.$$

Now by the definition of complex multiplication, $\alpha^\dagger$ acts as $\bar{\alpha}$. It therefore acts as the identity on $V_{\mathfrak{q}}$ for $\mathfrak{q}\neq\bar{\mathfrak{p}}$, and as multiplication by p on $V_{\bar{\mathfrak{p}}}$. So, by the same argument we have

$$\mathrm{ord}_p\det(\alpha^\dagger_{\mathcal{Y}_p(A/K)}) = \dim_{\mathbb{Q}_p} V_{\bar{\mathfrak{p}}},$$

and by Lemma 10 the result follows. □

Proof of Theorem. It suffices to show that $\dim_{\mathbb{Q}_p}\mathcal{Y}_p(A/K) = \sum_{\mathfrak{p}|p}\dim_{\mathbb{Q}_p} V_{\mathfrak{p}}$ is even. Let L be the fixed field of complex conjugation on M. If $\mathfrak{p}$ is inert or ramified in M/L, then $[M_{\mathfrak{p}} : \mathbb{Q}_p]$ is even. Therefore,

$$\dim_{\mathbb{Q}_p} V_{\mathfrak{p}} = [M_{\mathfrak{p}} : \mathbb{Q}_p]\dim_{M_{\mathfrak{p}}} V_{\mathfrak{p}}$$

is also even.

For the primes $\mathfrak{p}$ that split in M/L, we have $\mathfrak{p} \neq \bar{\mathfrak{p}}$, and, by Lemma 11,

$$\dim_{\mathbb{Q}_p} V_{\mathfrak{p}} = \dim_{\mathbb{Q}_p} V_{\bar{\mathfrak{p}}}.$$

Thus, $\sum_{\mathfrak{p}|p} \dim_{\mathbb{Q}_p} V_{\mathfrak{p}}$ is even, and so is $\mathrm{rk}_p(A/K)$. □

Remark 12. The complex multiplication assumption can be weakened. Suppose A is an abelian variety with $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q} \supset M$, for some field M, and suppose the Rosati involution induces a non-trivial automorphism on M. Then we can still show that $\mathrm{rk}_p(A)$ is even. Here denote this automorphism by $\phi \mapsto \bar{\phi}$, and the fixed field of it plays the role of L. Then the proof proceeds in the same way.

Remark 13. A similar argument can also be applied directly to p^∞-Selmer groups instead of Ш_d. Let $X_p(A/K) = \mathrm{Hom}(\mathrm{Sel}_{p^\infty}(A/K), \mathbb{Q}_p/\mathbb{Z}_p)$ and $\mathcal{X}_p(A/K) = X_p(A/K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Note that the $\mathbb{Q}_p$-rank of $\mathcal{X}_p(A/K)$ is $\mathrm{rk}_p(A/K)$. Then replace Theorem 5 with Theorem 7 from [3]. This tells us that for any self-isogeny ϕ, $Q(\phi) = Q(\hat{\phi})$, where, for an isogeny $\psi : A \to B$,

$$Q(\psi) := \#\mathrm{coker}(\psi : A(K)/A(K)_{\mathrm{tors}} \to B(K)/B(K)_{\mathrm{tors}})\#\ker(\psi_{\text{Ш}_d}).$$

Section 2 of [2] tells us that

$$\mathrm{ord}_p Q(\phi) = \mathrm{ord}_p \#\mathrm{coker}(\phi : X_p(A/K) \to X_p(A/K)).$$

By the same arguments as in the proof of Lemma 10, with Y_p and $\mathcal{Y}_p$ replaced by X_p and $\mathcal{X}_p$, we can show that for any invertible $\phi \in \mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}_p$,

$$\mathrm{ord}_p \det(\phi_{\mathcal{X}_p}) = \mathrm{ord}_p \det(\hat{\phi}_{\mathcal{X}_p}) = \mathrm{ord}_p \det(\phi^\dagger_{\mathcal{X}_p}).$$

Here, $\phi_{\mathcal{X}_p}$ denotes the map on $\mathcal{X}_p$ induced by ϕ. Then by an argument similar to Lemma 11 and the surrounding discussion, $\mathrm{rk}_p(A/K) = \dim_{\mathbb{Q}_p}(\mathcal{X}_p(A/K))$ is even.

ACKNOWLEDGEMENTS

I would like to thank my supervisor Vladimir Dokchitser for suggesting this problem, and for his advice and guidance. I would also like to thank the reviewers for their comments, and their help in strengthening the result. This work was supported by the Engineering and Physical Sciences Research Council [EP/S021590/1], the EPSRC Centre for Doctoral Training in Geometry and Number Theory (The London School of Geometry and Number Theory) at University College London.

JOURNAL INFORMATION

The *Bulletin of the London Mathematical Society* is wholly owned and managed by the London Mathematical Society, a not-for-profit Charity registered with the UK Charity Commission. All surplus income from its publishing programme is used to support mathematicians and mathematics research in the form of research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

ORCID

Jamie Bell https://orcid.org/0000-0002-6361-2237

REFERENCES

1. K. Česnavičius, *The p-parity conjecture for elliptic curves with a p-isogeny*, J. Reine Angew. Math. **2016** (2016), no. 719, 45–73.
2. T. Dokchitser and V. Dokchitser, *Self-duality of Selmer groups*, Math. Proc. Cambridge Philos. Soc. **146** (2009), 257–267.
3. T. Dokchitser and V. Dokchitser, *On the Birch–Swinnerton-Dyer quotients modulo squares*, Ann. Math. **172** (2010), 567–596.
4. T. Dokchitser and V. Dokchitser, *Root numbers and parity of ranks of elliptic curves*, J. Reine Angew. Math. **2011** (2011), no. 658, 39–64.
5. H. Green and C. Maistret, *The 2-parity conjecture for elliptic curves with isomorphic 2-torsion*, *Proc. R. Soc. A*, vol. 478, 2022, DOI 10.1098/rspa.2022.0112.
6. J. S. Milne, *Arithmetic duality theorems*, Second Edition, BookSurge, 2006.
7. J. Nekovář, *Compatibility of arithmetic and algebraic local constants (the case $l \neq p$)*, Compos. Math. **151** (2015), no. 9, 1626–1646.
8. E. Selmer, *A conjecture concerning rational points on cubic curves*, Math. Scand. **2** (1954), no. 1, 49–54.
9. J. S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177–190.