A. Shnidman. (0000) "Quadratic twists of abelian varieties with real multiplication,"
International Mathematics Research Notices, Vol. 0000, Article ID rnn000, 19 pages.
doi:10.1093/imrn/rnn000

Quadratic twists of abelian varieties with real multiplication

Ari Shnidman[1]

[1]Einstein Institute of Mathematics
The Hebrew University of Jerusalem
Edmond J. Safra Campus, Jerusalem, 91904, Israel

Correspondence to be sent to: ariel.shnidman@mail.huji.ac.il

Let F be a totally real number field and A/F an abelian variety with real multiplication by the ring of integers $\mathcal{O}$ of a totally real field. Assuming A admits an $\mathcal{O}$-linear 3-isogeny over F, we prove that a positive proportion of the quadratic twists A_d have rank 0. If moreover A is principally polarized and $Ш(A_d)$ is finite, then a positive proportion of A_d have $\mathcal{O}$-rank 1. Our proofs make use of the geometry-of-numbers methods from our previous work with Bhargava, Klagsbrun, and Lemke Oliver, and develop them further in the case of real multiplication.
We quantify these results for $A/\mathbb{Q}$ of prime level, using Mazur's study of the Eisenstein ideal. For example, suppose $p \equiv 10$ or $19 \pmod{27}$, and let A be the unique optimal quotient of $J_0(p)$ with a rational point P of order 3. We prove that at least 25% of twists A_d have rank 0 and the average $\mathcal{O}$-rank of $A_d(F)$ is at most $7/6$. Using the presence of two different 3-isogenies in this case, we also prove that roughly $1/8$ of twists of the quotient $A/\langle P\rangle$ have non-trivial 3-torsion in their Tate-Shafarevich groups.

1 Introduction

As part of his study of the modular Jacobians, Mazur showed that there are geometrically simple abelian varieties $A/\mathbb{Q}$ of arbitrarily large dimension having finite Mordell-Weil group Mazur [1977]. The existence of such abelian varieties also follows from combining results of Gross-Zagier, Kolyvagin-Logachev, and Bump-Friedberg-Hoffstein Bump et al. [1990], Gross and Zagier [1986], Kolyvagin and Logachëv [1989]. These examples are obtained by considering quadratic twists of simple quotients of the modular Jacobian $J_0(N)$.

Of course, one expects more than the mere *existence* of such abelian varieties. Presumably, a significant *proportion* of abelian varieties should have rank 0. Unfortunately, it is hard to prove quantitative results in this direction. Indeed, it was only recently that Bhargava and Shankar proved that a positive proportion of elliptic curves over $\mathbb{Q}$ have rank 0 Bhargava and Shankar [2015]. Geometry-of-numbers methods have since been deployed to study various algebraic families of abelian varieties of higher dimension Bhargava and Gross [2013], Bhargava et al. [2017], Bhargava et al., Poonen and Stoll [2014], Shankar [2019], leading us to ask:
Question 1. Is there a non-trivial, algebraic family of abelian varieties of dimension $g > 1$ over $\mathbb{Q}$ for which a positive proportion of members are geometrically simple and have rank 0? □

In this article, we provide a large class of such families. Our examples are quadratic twist families of quotients of $J_0(N)$, and the proof is via 3-Selmer groups and the geometry of numbers. Our method gives a lower bound on the proportion of rank 0 twists that is, in principle, explicit. For example, for certain optimal quotients of $J_0(p)$, we show that at least 25% of twists have rank 0; see Theorem 1.5 below.

We remark that the recent methods of Kriz-Li Kriz and Li [2019] could also be used to give affirmative answers to Question 1. Their approach uses congruences of modular forms, and originates in work of Vatsal Vatsal [1999] and ultimately Mazur himself Mazur [1979].

Received 26 February 2019
Communicated by <Editor communicating this article>

1.1 Real multiplication

To make our results more precise, let F be a number field, and A an abelian variety over F of dimension g. Let K be a totally real number field of degree g over $\mathbb{Q}$, and let $\mathcal{O}$ be a subring of finite index in the ring of integers $\mathcal{O}_K$. We say A has *real multiplication* (RM) by $\mathcal{O}$ if there is an embedding $\iota\colon \mathcal{O} \hookrightarrow \mathrm{End}_F(A)$.

Any elliptic curve has RM by $\mathbb{Z}$. But among abelian varieties of dimension greater than 1, those with RM are quite special. First of all, they lie on proper closed subvarieties (Hilbert modular varieties) of the moduli space of polarized abelian varieties. More importantly, their arithmetic parallels the arithmetic of elliptic curves, in certain respects. For example, if $F = \mathbb{Q}$, then it follows from results of Khare-Wintenberger and Ribet Khare and Wintenberger [2009], Ribet [1992] that A is a quotient of a modular Jacobian $J_0(N)$ for some N.

We will consider abelian varieties A with RM by $\mathcal{O}$ and with an additional bit of level structure. We say A *admits an $\mathcal{O}$-linear 3-isogeny* if there is another abelian variety B with RM by $\mathcal{O}$, and an $\mathcal{O}$-equivariant 3-isogeny $\phi\colon A \to B$ over F. The kernel of ϕ is then an $\mathcal{O}$-module scheme which is annihilated by an ideal I of index 3 in $\mathcal{O}$. We call I the *kernel ideal* of ϕ.*

1.2 General results

For each $d \in F^\times/F^{\times 2}$, we write A_d for the twist of A by the character $\chi_d\colon \mathrm{Gal}(\bar{F}/F) \to \{\pm 1\}$ corresponding to the extension $F(\sqrt{d})/F$. There is a *height* function on $F^\times/F^{\times 2}$, given by

$$H(d) = \prod_{\mathfrak{p}\colon \mathrm{ord}_{\mathfrak{p}}(d) \text{ odd}} N(\mathfrak{p}),$$

the product being over finite places $\mathfrak{p}$ of F. This gives an ordering of the quadratic twist family and allows us to define the *average* of a function $f\colon F^\times/F^{\times 2} \to \mathbb{R}$, as follows

$$\mathrm{avg}_d f(d) = \lim_{X\to\infty} \frac{\sum_{H(d)<X} f(d)}{\sum_{H(d)<X} 1}.$$

Similarly, when we say a positive proportion of twists A_d satisfy a certain property, we mean with respect to the height function H on $d \in F^\times/F^{\times 2}$.

Our first result answers Question 1 affirmatively, and provides a large class of examples.

Theorem 1.1. Let F be a totally real number field, and let A be an abelian variety over F with RM by $\mathcal{O}$. Suppose A admits an $\mathcal{O}$-linear 3-isogeny whose kernel ideal I is an invertible $\mathcal{O}$-module. Then a positive proportion of twists A_d have rank 0. □

In Theorem 1.5 and Section 7 we give examples of A satisfying the hypotheses of Theorem 1.1. For now, we simply note that I is automatically invertible if $3 \nmid [\mathcal{O}_K\colon \mathcal{O}]$ or if I is principal.

Theorem 1.1 gives the first progress in dimension $g > 1$ towards the following extension of Goldfeld's conjecture Goldfeld [1979] for quadratic twists of elliptic curves over $\mathbb{Q}$.

Conjecture 1.2. Let $A/\mathbb{Q}$ be a simple quotient of $J_0(N)$ of dimension g. Then 50% of twists A_d have rank 0, and 50% of twists A_d have rank g. □

Note that the rank of $A(\mathbb{Q})$ is a multiple of g, since $A(\mathbb{Q})$ is an $\mathcal{O}$-module. On the analytic side, $L(A, s)$ is the product of g conjugate automorphic L-functions. Thus, Goldfeld's minimalist philosophy and the conjecture of Birch and Swinnerton-Dyer lead directly to Conjecture 1.2.

Our next result concerns the quadratic twists with rank equal to g, or in other words, the twists with $\mathcal{O}$-rank equal to 1. It is conditional on the finiteness of the Tate-Shafarevich group, but we prove an unconditional result on the ranks of certain Selmer groups defined in Section 4.

Theorem 1.3. Let A and I be as in Theorem 1.1, and let $\pi\colon A \to A/A[I]$ be the natural $(3,3)$-isogeny. Suppose A admits an $\mathcal{O}$-linear polarization λ with $3 \nmid \deg(\lambda)$. Then a positive proportion of twists A_d satisfy $\dim_{\mathbb{F}_3} \mathrm{Sel}_\pi(A_d) = 1$. If $Ш(A_d)$ is finite for all d, then for a positive proportion of A_d, the $\mathcal{O}$-module $A_d(F)$ has rank 1. □

*This terminology is used in Waterhouse [1969], but with a slightly different meaning.

In the elliptic curve case $g = 1$, Theorems 1.1 and 1.3 were proven by Bhargava, Klagsbrun, Lemke Oliver, and the author [Bhargava et al., Thm. 1.6]. And indeed, a key ingredient in the proofs of Theorem 1.1 and 1.3 is the general result [Bhargava et al., Thm. 1.1], which determines the average size of the Selmer groups $\mathrm{Sel}_{\phi_d}(A_d)$, where $\phi_d\colon A_d \to A'_d$ is the quadratic twist family of *any* 3-isogeny $\phi\colon A \to A'$ of abelian varieties. The other two main ingredients are an analysis of Selmer groups in '$\mathcal{O}$-isogeny chains' of RM abelian varieties, and a collection of arithmetic duality theorems. These two ingredients reduce our task to controlling a single 3-isogeny, as opposed to simultaneously controlling the average behavior of a chain of 3-isogenies. When $F = \mathbb{Q}$, the result on twists of $\mathcal{O}$-rank 1 can presumably be made unconditional using the methods of Kriz-Li [Kriz and Li, 2019, Thm. 7.1].

Our method also leads to the following explicit upper bound on the average rank of $A_d(F)$. This greatly improves the bound implicitly given in Bhargava et al. for a general abelian variety A admitting an endomorphism which factors into 3-isogenies.

Theorem 1.4. Let A be as in Theorem 1.1, and let $\phi_d\colon A_d \to B_d$ be the corresponding family of $\mathcal{O}$-linear 3-isogenies. Then the average $\mathcal{O}$-rank of the quadratic twists A_d, for $d \in F^\times/F^{\times 2}$, is at most $\mathrm{avg}_d\left(t(\phi_d) + 3^{-t(\phi_d)}\right)$, where $t(\phi_d)$ is the absolute log-Selmer ratio of ϕ_d. □

The average here is computed with respect to the height function $H(d)$ on $F^\times/F^{\times 2}$. See Section 5 for the definition of the absolute log-Selmer ratio. If $\dim A = 1$, then this is [Bhargava et al., Thm. 1.4].

Theorem 1.4 is explicit in the sense that the stated upper bound can be easily computed if one knows the Tamagawa ratios $c_\ell(B_d)/c_\ell(A_d)$, for each prime ℓ and each twist d. With this data, one can also give an explicit lower bound on the proportion of rank 0 (resp. π-Selmer rank 1) twists; see Theorems 5.4 and 5.5. Our next result gives a class of abelian varieties A for which we obtain explicit and uniform bounds.

1.3 Optimal quotients of $J_0(p)$

Let $p \geq 5$ be a prime. Mazur's Theorem 1 Mazur [1977] states that the torsion subgroup of $J_0(p)$ is cyclic of order equal to the numerator of $\frac{p-1}{12}$. Thus, if $p \equiv 1 \pmod 9$, then $J_0(p)$ has a rational point of order 3. Recall that an *optimal quotient* of $J = J_0(p)$ is an abelian variety of the form $J/I_f J$ for some newform f on $\Gamma_0(p)$; here $I_f \subset \mathbb{T}$ is the kernel of the map $\mathbb{T} \to \mathbb{C}$ giving the action of the Hecke algebra on f. By a result of Emerton [Emerton, 2003, Thm. B], at least one optimal quotient of $J_0(p)$ also has a point of order 3. If moreover $p \not\equiv 1 \pmod{27}$, then this optimal quotient is unique.

We show that our general results apply to such optimal quotients, and we make explicit the bounds in Theorems 1.1, 1.3, and 1.4. The bounds turn out to be quite strong and are uniform in p:

Theorem 1.5. Suppose $p \equiv 10$ or $19 \pmod{27}$. Let $A/\mathbb{Q}$ be the unique optimal quotient of $J_0(p)$ with a rational point P of order 3 and let $\phi\colon A \to B = A/\langle P\rangle$ be the natural 3-isogeny. Then

(*a*) the average $\mathcal{O}$-rank of $A_d(\mathbb{Q})$ is at most $\frac{7}{6}$,

(*b*) at least $\frac{1}{4}$ of twists A_d, have rank 0 and even absolute log-Selmer ratio,

(*c*) at least $\frac{5}{12}$ of twists satisfy $\mathrm{rk}_{\mathcal{O}}\, A_d(\mathbb{Q}) \leq 1$, and have odd absolute log-Selmer ratio, and

(*d*) at least $\frac{1}{8}\frac{p}{p+1}$ of twists satisfy $\dim_{\mathbb{F}_3} Ш(B_d)[3] \geq 2$.

If A admits a prime-to-3 polarization and if $Ш(A_d)$ is finite, then $\mathrm{rk}_{\mathcal{O}} A_d(\mathbb{Q}) = 1$ in (*c*). □

The proof of Theorem 1.5 makes use of the rich arithmetic of $J_0(p)$ in several crucial ways. We first use the local principality of the Eisenstein ideal Mazur [1977] to verify that the kernel ideal of ϕ is invertible. We then use a result of Emerton Emerton [2003] to compute the ratio of the Tamagawa numbers $c_p(A_d)$ and $c_p(B_d)$. Finally, the average rank bound in (*a*) comes from a descent along a *different* 3-isogeny $\psi\colon A \to B'$, whose kernel is the image of the 3-part of the Shimura subgroup $\Sigma \subset J_0(p)$. The rank bound from ϕ is (on average) worse than the rank bound from ψ, which allows us to prove (*d*).

We emphasize that it is somewhat surprising that the bounds in Theorem 1.5 are uniform in p. Indeed, thinking locally at p, there are (a priori) several possibilities for the Tamagawa ratios $c_p(B)/c_p(A)$ and $c_p(B')/c_p(A)$. But it turns out that the *global* arithmetic of the prime level modular Jacobian forces both of these ratios to equal $1/3$. Our methods extend to squarefree level, whenever one can verify the invertibility of the kernel ideal. But since the global arithmetic is less constrained in composite levels, any general result using our approach will necessarily be less clean. We also note that the uniformity in prime level cannot be observed by restricting to elliptic curves, since A in Theorem 1.5 is an elliptic curve if and only if $p = 19$ or $p = 37$.

Finally, we remark that Theorem 1.5(d) gives the first known examples of geometrically simple abelian varieties over $\mathbb{Q}$ of dimension $g > 1$ with a positive proportion of quadratic twists having non-trivial elements in Ш. In Bhargava et al. [2019], the author, Bhargava, Klagsbrun, and Lemke Oliver give examples of this phenomenon for certain higher dimensional abelian varieties over number fields, but not over $\mathbb{Q}$.

1.4 Rational points on curves of genus $g \geq 2$

Finally, Theorem 1.1 also has consequences for the study of rational points in quadratic twist families of hyperelliptic curves C/F of genus $g \geq 2$. These families have the (affine) model $C_d\colon dy^2 = f(x)$, with f a polynomial of degree at least 5. For such families, it is natural to ask about the average size of $C_d(F)$, since $\#C_d(F) < \infty$. There are possibly 'trivial' rational points of the form $(\alpha, 0)$, where α is a root of $f(x)$, but Granville has conjectured that there are no other points, on average:

Conjecture 1.6 (Granville Granville [2007])**.** If C be a smooth hyperelliptic curve over $\mathbb{Q}$ of genus $g \geq 2$, then for 100% of $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, the set $C_d(\mathbb{Q})$ consists only of fixed points for the hyperelliptic involution. □

Granville gave a conditional proof in many cases, assuming the *abc*-conjecture Granville [2007], but there seems to be essentially no unconditional results towards this conjecture.[†] By considering curves with either a local obstruction or a map to an elliptic curve, one can easily construct families of curves with a large proportion of twists having no non-trivial points. So the most interesting case is when C has a rational Weierstrass point and absolutely simple Jacobian.

Our final result gives partial progress towards Conjecture 1.6.

Theorem 1.7. Let F be a totally real field and C a hyperelliptic curve over F. Assume $J = \mathrm{Jac}(C)$ has RM by $\mathcal{O}$ and admits an $\mathcal{O}$-linear 3-isogeny whose kernel ideal is an invertible $\mathcal{O}$-module. For a positive proportion of d, $C_d(F)$ consists entirely of points fixed by the hyperelliptic involution. □

Proof. By Theorem 1.1, we have $J_d(F) = J_d(F)_{\mathrm{tors}}$ for a positive proportion of d. As Galois-modules, we have $J(C_d)[n] \simeq J(C)[n] \otimes \chi_d$. Thus, $J(C_d)(F) = J(C_d)[2](F)$ for all but finitely many of these d. If $C_d(F)$ is non-empty, then $C_d(F) \hookrightarrow J_d(F)$ via the Abel-Jacobi map. Since the intersection $J(C_d)[2](F) \cap C_d(F)$ is the set of points fixed by the hyperelliptic involution, the theorem follows. ■

In forthcoming work, Bruin, Flynn, and the author give an explicit parameterization of the universal hyperelliptic curve with RM by $\mathbb{Z}[\sqrt{3}]$ and with $(\mathbb{Z}/3\mathbb{Z} \times \mu_3)$-level structure. This gives a large class of geometrically simple examples in genus 2 for which Theorem 1.7 applies, and one can make the proportion of twists in Theorem 1.7 explicit. In Section 7, we give some sporadic examples.

Theorem 1.7 therefore gives significant progress towards Conjecture 1.6 for many new curves. It would be interesting to try to incorporate the recent work of Balakrishnan-Dogra on non-abelian Chabauty for curves with RM Balakrishnan and Dogra [2019].

2 Abelian varieties with real multiplication

Let F be a number field. Also, let K be a totally real number field of degree $g \geq 1$ over $\mathbb{Q}$, and let $\mathcal{O}$ be a subring of finite index in the ring of integers $\mathcal{O}_K$.

2.1 Real multiplication and isogenies

Definition 2.1. A g-dimensional abelian variety A over F *has real multiplication by* $\mathcal{O}$ if there is an algebra embedding $\mathcal{O} \hookrightarrow \mathrm{End}_F(A)$. □

Let A be an abelian variety with real multiplication (RM) by $\mathcal{O}$, and fix $\mathcal{O} \hookrightarrow \mathrm{End}_F(A)$, so that we may think of elements of $\mathcal{O}$ as endomorphisms of A. Our goal is to study the ranks of the quadratic twists A_d, for d in $F^\times/F^{\times 2}$. Recall that A_d is the twist of A by the character $\chi_d\colon G_F \to \{\pm 1\}$ corresponding to $F(\sqrt{d})$; here $G_F = \mathrm{Gal}(\bar{F}/F)$.

Lemma 2.2. The abelian variety A_d has RM by $\mathcal{O}$, for all $d \in F^\times/F^{\times 2}$. More precisely, the embedding $\iota\colon \mathcal{O} \hookrightarrow \mathrm{End}_F(A)$ induces an embedding $\iota_d\colon \mathcal{O} \hookrightarrow \mathrm{End}_F(A_d)$. □

[†]For unconditional results in the family of *all* odd degree hyperelliptic curves, see the work of Poonen-Stoll Poonen and Stoll [2014].

Proof. Since the automorphism $-1 \in \mathrm{Aut}_F(A)$ commutes with action of $\mathcal{O} \subset \mathrm{End}_F(A)$, we see that the action of $\mathcal{O}$ on $A \otimes_F F(\sqrt{d}) \simeq A_d \otimes_F F(\sqrt{d})$ descends to A_d. ■

Since ι is fixed, we can safely consider $\alpha \in \mathcal{O}$ as an endomorphism of A and as an endomorphism of A_d, without any ambiguity.

In order to say something about the ranks of the twists A_d, we suppose from now on that A admits an $\mathcal{O}$-linear 3-isogeny. In other words, we assume there exists an abelian variety B which also has RM by $\mathcal{O}$ over F and a 3-isogeny $\phi\colon A \to B$ over F which is $\mathcal{O}$-equivariant. The kernel $A[\phi]$ is an $\mathcal{O}$-module scheme of order 3, and hence is annihilated by an ideal I in $\mathcal{O}$ of index 3. We call I the *kernel ideal* of ϕ. We have $A[\phi] \subset A[I]$.

Lemma 2.3. If $J \subset \mathcal{O}$ is an invertible $\mathcal{O}$-ideal of index p, for some prime p, then $A[J](\bar{F}) \simeq (\mathbb{Z}/p\mathbb{Z})^2$ as abelian groups. □

Proof. Since $A[J] \subset A[p]$, it is enough to show that $A[J]$ has order p^2. The claim is true if $J = (\epsilon)$ is a principal ideal. Indeed, since $[K\colon \mathbb{Q}] = \dim A$, we then have

$$\#A[J](\bar{F}) = \deg(\epsilon) = \mathrm{Nm}(\epsilon)^2 = p^2,$$

by [Mumford, 1970, §19]. Since J is invertible, there is an integer $k \geq 1$ such that J^k is principal, and the same argument shows that $\#A[J^k](\bar{F}) = p^{2k}$. The lemma now follows since $\#A[J^k](\bar{F}) = \#A[J](\bar{F})^k$. ■

By the Lemma, if I is invertible, then the natural quotient $\pi\colon A \to A/A[I]$ is a $(3,3)$-isogeny which factors through $\phi\colon A \to B$. Moreover, the quotient $C := A/A[I]$ also has RM by $\mathcal{O}$, and $\pi\colon A \to C$ is $\mathcal{O}$-linear.

Remark Conversely, if $I \subset \mathcal{O}$ is an invertible $\mathcal{O}$-ideal of index 3, and if the $(3,3)$-isogeny $A \to A/A[I]$ factors through a 3-isogeny $\phi\colon A \to B$, then B has RM by $\mathcal{O}$ and ϕ is necessarily $\mathcal{O}$-linear with kernel ideal I.

Let $\phi'\colon B \to C$ be the 3-isogeny over F such that $\pi = \phi' \circ \phi$. By Lemma 2.2, there are 3-isogenies $\phi_d\colon A_d \to B_d$ and $\phi'_d\colon B_d \to C_d$, such that $\phi'_d \circ \phi_d = \pi_d \in \mathrm{Hom}(A_d, C_d)$, for each $d \in F^\times/F^{\times 2}$. Note that

$$A_d[\phi_d] \simeq A[\phi] \otimes \chi_d \quad \text{and} \quad B_d[\phi'_d] \simeq B[\phi'] \otimes \chi_d \tag{2.1}$$

as $\mathbb{F}_3[G_F]$-modules.

2.2 Polarizations and duality

A *polarization* is a homomorphism $\lambda\colon A \to \hat{A}$ over F which, over $\bar{F}$, takes the form $\phi_L\colon A_{\bar{F}} \to \hat{A}_{\bar{F}}$ for some ample line bundle $L \in \mathrm{Pic}(A_{\bar{F}})$. If λ is an isomorphism, we call it a *principal polarization*.

In order to study the ranks of the twists A_d, we further impose:

Assumption Assume A admits an $\mathcal{O}$-linear 3-isogeny $\phi\colon A \to B$ over F, and that

1. F is a totally real field.
2. The kernel ideal I of ϕ is an invertible $\mathcal{O}$-module.
3. A admits an $\mathcal{O}$-linear polarization $\lambda\colon A \to \hat{A}$ over F of degree prime to 3.

These assumptions allow us to glean extra information on the group schemes $A[\pi]$, $A[\phi]$ and $B[\phi']$. For some of our results (e.g. Theorem 1.1) we will eventually be able to remove the assumption on the polarization via Zarhin's trick.

Proposition 2.4. The group scheme $A[\pi]$ is self-dual. □

Proof. Since I is an invertible $\mathcal{O}$-module, there exists an ideal J of $\mathcal{O}$ which is coprime to 3 and such that $(\alpha)I = (\beta)J$, for $\alpha, \beta \in \mathcal{O}$. It follows that $C = A/A[I]$ is also isomorphic to $A/A[J]$. Since J is prime to 3, we may fix an isogeny $\psi\colon C \to A$ of degree prime to 3 such that the composition $\psi \circ \pi$ lies in $\mathcal{O} \subset \mathrm{End}_F(A)$. By $\mathcal{O}$-linearity of λ, the following diagram is commutative:

$$\begin{array}{ccccc} A & \xrightarrow{\pi} & C & \xrightarrow{\psi} & A \\ \downarrow{\scriptstyle\lambda} & & & & \downarrow{\scriptstyle\lambda} \\ \widehat{A} & \xrightarrow{\widehat{\psi}} & \widehat{C} & \xrightarrow{\widehat{\pi}} & \widehat{A} \end{array}$$

Since $\deg(\lambda)$ and $\deg(\hat{\psi})$ are prime to 3, the kernel $A[\pi]$ maps isomorphically onto $\hat{C}[\hat{\pi}]$, and hence $A[\pi]$ is self-dual. ■

Proposition 2.5. For any $d \in F^\times/F^{\times 2}$, the group schemes $A_d[\phi_d]$ and $B_d[\phi'_d]$ are Cartier dual. □

Proof. We identify group schemes such as $A_d[\phi_d]$ and $B_d[\phi'_d]$ with their corresponding $\mathbb{F}_3[G_F]$-modules. Note that isomorphism classes of order 3 $\mathbb{F}_3[G_F]$-modules are in bijection with quadratic characters $\chi\colon G_F \to \{\pm 1\}$. Moreover, the Cartier dual of H corresponds to the character $\chi\chi_3$, where χ_3 is the character of μ_3. Thus by (2.1), we may reduce to the case $d = 1$ and drop subscripts.

Let χ and χ' be the quadratic characters corresponding to $A[\phi]$ and $B[\phi']$. These are the Jordan-Holder factors of $A[\pi]$. Since $A[\pi]$ is self-dual, we have the equality of multi-sets

$$\{\chi, \chi'\} = \{\chi\chi_3, \chi'\chi_3\},$$

since the right hand side is the set of Jordan-Holder factors of the dual of $A[\pi]$. As F is totally real, we have $\chi \neq \chi\chi_3$, and so we must have $\chi = \chi'\chi_3$. Thus $A[\phi]$ and $B[\phi']$ are Cartier dual. ■

Remark In fact, Proposition 2.5 holds over any F not containing $\sqrt{-3}$.

From the proof of the propositions, we obtain the following corollaries.
Corollary 2.6. There is an isogeny $A \to \hat{C}$ of degree prime to 3, which induces an isomorphism $A[\phi] \to \hat{C}[\hat{\phi}']$. In particular, there is an isomorphism $H^1(G_F, A[\phi]) \simeq H^1(G_F, \hat{C}[\hat{\phi}'])$. □
Corollary 2.7. The polarization λ induces an isogeny $\lambda_B\colon B \to \hat{B}$ of degree prime to 3. □

Proof. Using the notation from the proof of Proposition 2.4, the composition $\hat{\psi} \circ \lambda$, sends $A[\phi]$ isomorphically onto $\hat{C}[\hat{\phi}']$, and so the composition

$$B \simeq A/A[\phi] \to \hat{C}/\hat{C}[\hat{\phi}'] \simeq \hat{B},$$

gives the desired isogeny. ■

Corollary 2.8. The isogeny $\lambda_B\colon B \to \hat{B}$ is equal to its own dual. □

Proof. We give an alternate construction of λ_B. Let $\alpha = \psi \circ \pi \in \mathrm{End}_F(A)$. The $\mathcal{O}$-linearity of λ exactly means that α is fixed by the Rosati involution on $\mathrm{End}_F(A)$ associated to λ. Thus, the homomorphism $\lambda \circ \alpha\colon A \to \hat{A}$ is symmetric, i.e. equal to its own dual. It follows that over $\bar{F}$, we have $\lambda \circ \alpha = \phi_L$ for some line bundle L on $A_{\bar{F}}$.

We claim that L is of the form $\phi^* M$, for some line bundle M on $B_{\bar{F}}$. Indeed, by the theory of descent of line bundles on abelian varieties, it is enough to show that the (cyclic) group scheme $A[\phi]$ lies in the kernel of $\lambda \circ \alpha$, which is of course true since $A[\phi] \subset A[\pi]$. By degree considerations, it follows that the symmetric isogeny $\phi_M\colon B_{\bar{F}} \to \hat{B}_{\bar{F}}$ has degree $\deg(\lambda_B)$. By construction, we have $\phi_M = \hat{\phi}^{-1}\lambda\alpha\phi^{-1}$. Since ϕ, α, and λ are all defined over F, the map ϕ_M descends to a morphism $B \to \hat{B}$ over F, which is the isogeny λ_B defined earlier. ■

Remark *The symmetric isogeny $\lambda_B\colon B \to \hat{B}$ is not necessarily a polarization, even if $\deg(\lambda) = 1$ and I is principal (in which case $\deg(\lambda_B) = 1$). For example, if $K = \mathbb{Q}(\sqrt{3})$ with $\pi = \sqrt{3}$, then λ_B is not a polarization. On the other hand, if $K = \mathbb{Q}(\sqrt{6})$ with $\pi = 3 + \sqrt{6}$, then λ_B is a (principal) polarization. The difference is that $3 + \sqrt{6}$ is totally positive, while $\sqrt{3}$ is not. See [González et al., 2005, Thm. 2.10].*

2.3 Isogeny chains

Let $k \geq 1$ be the order of the class $[I]$ in $\mathrm{Pic}(\mathcal{O})$. Then $I^k = \epsilon\mathcal{O}$, for some $\epsilon \in \mathcal{O}$. We will also regard ϵ as an endomorphism of A. If J is any $\mathcal{O}$-ideal, then the quotient $A/A[J]$ has RM by $\mathcal{O}$. We may therefore recursively define

$$A_1 = A \quad \text{and} \quad A_i = A_{i-1}/A_{i-1}[I] \text{ for } i \geq 2.$$

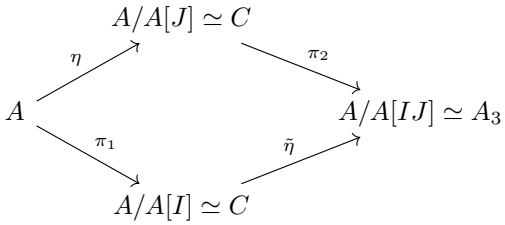
Note that $C = A_2$ and

$$A_{k+1} = A/A[I^k] = A/A[\epsilon] \simeq A,$$

so that $A_{k+i} \simeq A_i$ for all $i \geq 1$.

For $i \geq 1$, we define $\pi_i\colon A_i \to A_{i+1}$ to be the natural $(3,3)$-isogeny with kernel $A_i[I]$. In particular, $\pi_1 = \pi$ and $\epsilon = \pi_k\pi_{k-1}\cdots\pi_2\pi_1 \in \mathrm{End}_F(A)$. We also have $\pi_{k+i} = \pi_i$ for all $i \geq 1$.
Proposition 2.9. For each $i \geq 1$, there exists an isogeny $A_i \to A_{i+1}$ of degree prime to 3, which maps $A_i[\pi_i]$ isomorphically onto $A_{i+1}[\pi_{i+1}]$. □

Proof. We may immediately reduce to the case $i = 1$, so that $A_2 = C$. Since I is an invertible $\mathcal{O}$-module, we may choose an invertible $\mathcal{O}$-ideal J which is prime to 3 and in the same ideal class of I in $\mathrm{Pic}(\mathcal{O})$. Then $C \simeq A/A[J]$ and the quotients $\eta\colon A \to C = A/A[J]$ and $\tilde{\eta}\colon C \to A_3 \simeq C/C[J]$ have degrees prime to 3. The commutativity of the diagram



shows that η sends $A[\pi]$ isomorphically onto $C[\pi_2]$, as desired. ■

Corollary 2.10. Each $(3,3)$-isogeny $\pi_i\colon A_i \to A_{i+1}$ factors as a composition of 3-isogenies; hence the endomorphism $\epsilon\colon A \to A$ factors as a composition of 3-isogenies. □

Proof. Since $A[\pi_i] \simeq A[\pi]$, and $A[\pi]$ is reducible as $\mathbb{F}_3[G_F]$-module, so is $A[\pi_i]$. It follows that π_i factors into a pair of 3-isogenies. ■

Corollary 2.11. For each $i \geq 1$, there are isomorphisms $H^1(G_F, A_i[\pi_i]) \simeq H^1(G_F, A[\pi])$. □

Finally, note that the results in this section apply equally well if we replace A and B by A_d and B_d (as well as replacing the isogenies ϕ and ϕ' by ϕ_d and ϕ'_d), for any $d \in F^\times/F^{\times 2}$.

3 Local Selmer ratios

3.1 Generalities

For the first part of this section, we let $\phi\colon A \to B$ be any isogeny of abelian varieties over a number field F. We will recall the definitions of the local and global Selmer ratios attached to ϕ. One expects (and in certain special cases, one can prove) that these numbers dictate the average behavior of the ranks of the Selmer group $\mathrm{Sel}_\phi(A)$, as $\phi\colon A \to B$ varies through an algebraic family of isogenies. Assume, for simplicity, that the degree of ϕ is ℓ^n for some prime ℓ. Eventually we will take $\ell = 3$.

For each place $\mathfrak{p}$ of F, write $F_\mathfrak{p}$ for the completion at $\mathfrak{p}$. There is an induced homomorphism of groups $\phi^{(\mathfrak{p})}\colon A_d(F_\mathfrak{p}) \to B_d(F_\mathfrak{p})$, and the *local* Selmer ratio is defined to be

$$c_\mathfrak{p}(\phi) = \frac{\#\mathrm{coker}\,\phi^{(\mathfrak{p})}}{\#\ker\phi^{(\mathfrak{p})}}, \tag{3.1}$$

which lies in $\ell^{\mathbb{Z}}$.

We also define the *global* Selmer ratio $c(\phi) = \prod_\mathfrak{p} c_\mathfrak{p}(\phi)$, where the product is over all places of F, including the archimedean ones. The following proposition and its corollary show that this is a finite product, and hence the global Selmer ratio is well-defined [Schaefer, 1996, Lem. 3.8].

Proposition 3.1. If $\mathfrak{p}$ is a finite place of F, then

$$c_\mathfrak{p}(\phi) = \frac{c_\mathfrak{p}(B)}{c_\mathfrak{p}(A)} \cdot \gamma_{\phi,F_\mathfrak{p}},$$

where $c_\mathfrak{p}(A)$ is the Tamagawa number of A at $\mathfrak{p}$, and $\gamma^{-1}_{\phi,F_\mathfrak{p}}$ is the normalized absolute value of the determinant of the Jacobian matrix of partial derivatives of the map induced by ϕ on formal groups over $F_\mathfrak{p}$, evaluated at the origin. In particular, $\gamma_{\phi,F_\mathfrak{p}} = \ell^k$ for some integer $k \geq 0$. □

Corollary 3.2. If $\mathfrak{p}$ is a finite place of F not above ℓ, then $c_\mathfrak{p}(\phi) = c_\mathfrak{p}(B)/c_\mathfrak{p}(A)$. Hence if A has good reduction at $\mathfrak{p}$ and $\ell \nmid \mathfrak{p}$, then $c_\mathfrak{p}(\phi) = 1$. □

The local Selmer ratio at archimedean places of F is easy to compute:

Lemma 3.3. If $\mathfrak{p}$ is an archimedean place of F and if $\ell \neq 2$, then $c_\mathfrak{p}(\phi) = \#A[\phi](F_\mathfrak{p})^{-1}$. □

Proof. In this case, $\mathrm{coker}(\phi^{(F_\mathfrak{p})})$ is both a 2-group and an ℓ-group, so is trivial. ■

We will need some formal properties of local and global Selmer ratios.

Lemma 3.4. Let $\mathfrak{p}$ be a place of F and let $\phi\colon A \to B$ and $\psi\colon B \to C$ be isogenies of abelian varieties over $F_\mathfrak{p}$. Then $c_\mathfrak{p}(\psi\phi) = c_\mathfrak{p}(\psi)c_\mathfrak{p}(\phi)$. □

Proof. [Milne, 2006, I.7.2]. ■

Corollary 3.5. Let $\phi\colon A \to B$ and $\psi\colon B \to C$ be isogenies of abelian varieties over F. Then $c(\psi\phi) = c(\psi)c(\phi)$. □

Lemma 3.6. Suppose $\phi\colon A \to B$ and $\psi\colon B \to C$ are isogenies over F_p for some place $\mathfrak{p}$ of F. Then $\gamma_{\psi\phi,F_\mathfrak{p}} = \gamma_{\phi,F_\mathfrak{p}} \cdot \gamma_{\psi,F_\mathfrak{p}}$. □

Proof. This follows from Lemma 3.4 and Proposition 3.1. ■

Lemma 3.7. Let $\mathcal{O}$ be the ring of integers in a totally real field, and suppose A has RM by $\mathcal{O}$. Let $\alpha \in \mathcal{O}$ be an element of norm ℓ^n for some n. Suppose also that $\mathfrak{p}$ is a place of F dividing ℓ. Then $\gamma_{\alpha,F_\mathfrak{p}} = \ell^{n[F_\mathfrak{p}\colon \mathbb{Q}_\ell]}$. □

Proof. The case $\alpha \in \mathbb{Z}$ is proved in [Schaefer, 1996, Prop. 3.9], and the case of general α is proved in exactly the same way. Note that it is important here that α is an isogeny, which follows from the fact that the embedding $\mathcal{O} \hookrightarrow \mathrm{End}_F(A)$ sends 1 to 1_A. ■

3.2 RM isogeny chains

We return to the setup of the previous section, so that $\phi\colon A \to B$ is an $\mathcal{O}$-linear 3-isogeny of abelian varieties with RM by $\mathcal{O}$ over F. We also impose Assumption 2.2. Recall that I is the kernel ideal of ϕ and $\pi\colon A \to C = A/A[I]$ is the natural $(3,3)$-isogeny. Also recall from Section 2.3 the endomorphism $\epsilon\colon A \to A$ as well as the chain of $(3,3)$-isogenies $\pi_i\colon A_i \to A_{i+1}$ for $i \geq 1$.

Proposition 2.5 allows us to compute various local and global Selmer ratios in this setting.

Lemma 3.8. If $\mathfrak{p}$ is an archimedean place of F, then $c_\mathfrak{p}(\pi_i) = \frac{1}{3}$, for all i. □

Proof. It is enough to prove the statement for $\pi_1 = \pi$. There are only two group schemes of rank 3 over $\mathbb{R}$, namely $\mathbb{Z}/3\mathbb{Z}$ and μ_3, and they are dual to each other. Thus, by Proposition 2.5, one of $A[\phi]$ and $B[\phi']$ is isomorphic to μ_3 and the other is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ (over $F_\mathfrak{p}$). So $A[\pi]$ is either an extension of μ_3 by $\mathbb{Z}/3\mathbb{Z}$ or an extension of $\mathbb{Z}/3\mathbb{Z}$ by μ_3. In the former case, we clearly have $\#A[\pi](F_\mathfrak{p}) = 3$, which shows that $c_\mathfrak{p}(\pi) = \frac{1}{3}$, by Lemma 3.3. In the latter case, we have

$$0 \to \mu_3 \to A[\pi] \to \mathbb{Z}/3\mathbb{Z} \to 0$$

over $F_\mathfrak{p} \simeq \mathbb{R}$. Since $H^1(\mathrm{Gal}(\bar{\mathbb{R}}/\mathbb{R}), \mu_3) \simeq \mathbb{R}^\times/\mathbb{R}^{\times 3} = 0$, we see that $\#A[\pi](F_\mathfrak{p}) = 3$, and we again have $c_\mathfrak{p}(\pi) = \frac{1}{3}$. ■

Lemma 3.9. For each $i \geq 1$ and every place $\mathfrak{p}$ of F, we have $c_\mathfrak{p}(\pi_i) = c_\mathfrak{p}(\pi)$. □

Proof. This follows from Proposition 2.9. ■

Proposition 3.10. We have $c(\pi) = 1$ and $c(\epsilon) = 1$. □

For the proof, we introduce some notation. For any isogeny f of abelian varieties over F, and for any place p of $\mathbb{Q}$, we define $c_p(f) = \prod_{\mathfrak{p}|p} c_\mathfrak{p}(f)$, where the product is over the places of F over p.

Proof. The endomorphism $\epsilon\colon A \to A$ is an isogeny of degree 3^{2k}. By Proposition 3.1, we have $c_\mathfrak{p}(\epsilon) = 1$ for all finite $\mathfrak{p} \nmid 3$. Thus, by Lemmas 3.4, 3.6, 3.7, and 3.8, we have

$$c(\epsilon) = c_3(\epsilon)c_\infty(\epsilon) = 3^{k[F\colon \mathbb{Q}]}3^{-k[F\colon \mathbb{Q}]} = 1.$$

On the other hand, by Lemma 3.9, we have $c(\pi_i) = c(\pi)$ for all i. Thus,

$$1 = c(\epsilon) = \prod_{i=i}^{k} c(\pi_i) = c(\pi)^k,$$

which shows that $c(\pi) = 1$, as claimed. ■

Remark For an alternate proof use Proposition 2.4 and Theorem 4.2 below.
Corollary 3.11. We have $c(\phi') = c(\phi)^{-1}$. □

Proof. This follows from Corollary 3.5 and Proposition 3.10. ■

4 Poitou-Tate duality and parity of the π-Selmer rank

An isogeny $\psi\colon A \to A'$ of abelian varieties over a field F, gives rise to a short exact sequence

$$0 \to A[\psi] \to A \to A' \to 0$$

of group schemes over F, which we will also view as a short exact sequence of G_F-modules. Taking the long exact sequence in group cohomology gives the Kummer map $A'(F) \to H^1(F, A[\psi])$. If F is a number field, then the ψ-Selmer group $\mathrm{Sel}_\psi(A)$ is defined to be the subgroup of $H^1(F, A[\psi])$ consisting of cohomology classes whose restriction to $H^1(F_\mathfrak{p}, A[\psi])$ lies in the image of the Kummer map $A'(F_\mathfrak{p}) \to H^1(F_\mathfrak{p}, A[\psi])$, for all places $\mathfrak{p}$ of F.

We now place ourselves in the context of the previous sections, so that A is an abelian variety over a totally real field F satisfying Assumption 2.2. For each $d \in F^\times/F^{\times 2}$ we have the 3-isogenies $\phi_d\colon A_d \to B_d$ and $\phi'_d\colon B_d \to C_d$, whose composition is the $(3,3)$-isogeny $\pi\colon A_d \to C_d$; we purposely omit the subscript d from π because there will be no ambiguity. Each of the Selmer groups $\mathrm{Sel}_{\phi_d}(A_d)$, $\mathrm{Sel}_{\phi'_d}(B_d)$ and $\mathrm{Sel}_\pi(A_d)$ is a finite dimensional vector space over $\mathbb{F}_3$.

For each twist A_d, we have also defined the isogeny chain $\pi_i\colon A_{d,i} \to A_{d,i+1}$ for $i \geq 1$, with $\pi = \pi_1$ and $A_{d,i} = A_d$. Moreover the Selmer groups for the different π_i are all isomorphic:
Proposition 4.1. For each $i \geq 1$, we have $\mathrm{Sel}_{\pi_i}(A_{d,i}) \simeq \mathrm{Sel}_{\pi_{i+1}}(A_{d,i+1})$. □

Proof. This is a tedious but simple diagram chase using the isogenies guaranteed by Proposition 2.9 and the definition of the Selmer group. We note that these isomorphisms are not quite canonical, as they depend on the choice of isomorphisms in Proposition 2.9. ■

The purpose of this section is to collect some results which show that the global Selmer ratio $c(\phi_d)$ encodes important information concering the $\mathbb{F}_3$-ranks of these three Selmer groups. The key input is Poitou-Tate global duality. In the case of elliptic curves, these results are due to Cassels Cassels [1965].
Theorem 4.2. For A and B as above, we have

$$c(\phi) = \frac{\#\mathrm{Sel}_\phi(A)}{\#\mathrm{Sel}_{\phi'}(B)} \cdot \frac{\#B[\phi'](F)}{\#A[\phi](F)}.$$

□

Proof. For each place $\mathfrak{p}$ of F, the subgroup of local conditions in $H^1(F_\mathfrak{p}, B[\phi'])$ defining $\mathrm{Sel}_{\phi'}(B)$ is orthogonal under local Tate duality to the local conditions in $H^1(F_\mathfrak{p}, \hat{C}[\hat{\phi}'])$ defining $\mathrm{Sel}_{\hat{\phi}'}(\hat{C})$, by [Česnavičius, 2017, Prop. B.1]. Thus, by Wiles' duality formula [Neukirch et al., 2008, Thm. 8.7.9], we have

$$c(\hat{\phi}') = \frac{\#\mathrm{Sel}_{\hat{\phi}'}(\hat{C})}{\#\mathrm{Sel}_{\phi'}(B)} \cdot \frac{\#B[\phi'](F)}{\#\hat{C}[\hat{\phi}'](F)}.$$

On the other hand, by Corollary 2.6, we have $\mathrm{Sel}_\phi(A) \simeq \mathrm{Sel}_{\hat{\phi}'}(\hat{C})$, $c(\phi) = c(\hat{\phi}')$, and $A[\phi] \simeq \hat{C}[\hat{\phi}']$, from which we deduce the desired formula. ■

The next result is presumably well-known to experts, but we could not find it in the literature. This is a generalization of a result Cassels used to prove the non-degeneracy of the Cassels-Tate pairing for elliptic curves. Recall that the Cassels-Tate pairing for B is a pairing [Milne, 2006, Prop. I.6.9]

$$\langle\,,\,\rangle_B\colon Ш(B) \times Ш(\hat{B}) \to \mathbb{Q}/\mathbb{Z}.$$

Using the isogeny $\lambda_B\colon B \to \hat{B}$ from Corollary 2.7, we construct a bilinear pairing

$$\langle\,,\,\rangle_{\lambda_B}\colon Ш(B) \times Ш(B) \to \mathbb{Q}/\mathbb{Z}$$

defined by $\langle a, b\rangle_\lambda = \langle a, \lambda_B(b)\rangle_B$.

Theorem 4.3. Suppose $b \in Ш(B)[\phi']$. Then b is in the image of $\phi\colon Ш(A) \to Ш(B)$ if and only if $\langle b, b' \rangle_{\lambda_B} = 0$ for all $b' \in Ш(B)[\phi']$. □

Proof. This is proved exactly as in [Fisher, 2003, Thm. 3], using the fact that $H^1(G_F, A[\phi])$ and $H^1(G_F, B[\phi'])$ are in local duality by Corollary 2.6. See also the proof of [Milne, 2006, Lem. I.6.17]. ■

Theorem 4.3 will be used in the proof of the following theorem.
Theorem 4.4. If $c(\phi) = 3^m$, then $\dim_{\mathbb{F}_3} \mathrm{Sel}_\pi(A) \equiv m \pmod 2$. □

Proof. A diagram chase gives the following well-known five-term exact sequence

$$0 \to B(F)[\phi']/\phi(A(F)[\pi]) \to \mathrm{Sel}_\phi(A) \to \mathrm{Sel}_\pi(A) \to \mathrm{Sel}_{\phi'}(B) \to \frac{Ш(B)[\phi']}{\phi(Ш(A)[\pi])} \to 0. \tag{4.1}$$

Combining this with Theorem 4.2, we reduce to showing that

$$\dim_{\mathbb{F}_3} \frac{Ш(B)[\phi']}{\phi(Ш(A)[\pi])}$$

is even. But by Theorem 4.3, the Cassels-Tate pairing $\langle\, , \rangle_{\lambda_B}$ on $Ш(B)$ restricts to a non-degenerate pairing on this finite group. Moreover, the pairing is anti-symmetric by [Poonen and Stoll, 1999, Cor. 6]; here we use that A admits a prime-to-3 polarization. Since any anti-symmetric pairing on an $\mathbb{F}_3$-vector space is also alternating, it follows from the non-degeneracy that $Ш(B)[\phi']/\phi(Ш(A)[\pi])$ has even $\mathbb{F}_3$-rank, as desired. ■

Finally, we note that the theorems in this section apply equally well if we replace A and B by A_d and B_d (as well as replacing the isogenies ϕ and ϕ' by ϕ_d and ϕ'_d) for any $d \in F^\times/F^{\times 2}$.

5 Ranks of the quadratic twists A_d

We again place ourselves in the setting of Section 2 and Assumption 2.2. Recall the height function on $d \in F^\times/F^{\times 2}$ from the introduction:

$$H(d) = \prod_{\mathfrak{p}\colon \mathrm{ord}_\mathfrak{p}(d) \text{ is odd}} N(\mathfrak{p}),$$

where the product is over the finite primes of F. Having already defined the average value of a function on $F^\times/F^{\times 2}$, with respect to H, we define the *density* of a subset $\Sigma \subset F^\times/F^{\times 2}$ to be

$$\mu(\Sigma) = \mathrm{avg}_d\, 1_\Sigma(d),$$

where 1_Σ is the characteristic function of Σ.

We say Σ is defined by *finitely many local conditions* if there exists for each place $\mathfrak{p}$ of F subsets $\Sigma_\mathfrak{p} \subset F_\mathfrak{p}^\times/F_\mathfrak{p}^{\times 2}$, such that $\Sigma_\mathfrak{p} = F_\mathfrak{p}^\times/F_\mathfrak{p}^{\times 2}$ for all but finitely many $\mathfrak{p}$ and such that

$$\Sigma = F^\times/F^{\times 2} \bigcap \prod_\mathfrak{p} \Sigma_p,$$

with the intersection taking place inside $\prod_\mathfrak{p} F_\mathfrak{p}^\times/F_\mathfrak{p}^{\times 2}$. The average of a function f on Σ (ordered by the height function H) is denoted $\mathrm{avg}_\Sigma f(d)$.

The key input for our proofs of Theorems 1.1 and 1.3 is the following general result of Bhargava, Klagsbrun, Lemke Oliver, and the author [Bhargava et al., Thm. 1.1].
Theorem 5.1. Suppose $\psi\colon A \to A'$ is a degree 3 isogeny of abelian varieties over a number field F, and let $\psi_d\colon A_d \to A'_d$ be the corresponding quadratic twist family of 3-isogenies, for $d \in F^\times/F^{\times 2}$. If $\Sigma \subset F^\times/F^{\times 2}$ is a subset defined by finitely many local conditions, then the average size of $\mathrm{Sel}_{\psi_d}(A_d)$, for $d \in \Sigma$ is $1 + \mathrm{avg}_\Sigma\, c(\psi_d)$. □

Now assume that A is abelian variety over a totally real field F satisfying Assumption 2.2. For $m \in \mathbb{Z}$, we define the subsets

$$T_m(\phi) = \left\{ d \in F^\times/F^{\times 2} \colon c(\phi_d) = 3^m \right\} \subset F^\times/F^{\times 2}.$$

Then the sets $T_m(\phi)$ are defined by finitely many local conditions, and for any fixed m, either $T_m(\phi)$ is empty or it has positive density. We also write $T_{\pm m}(\phi)$ for $T_m(\phi) \cup T_{-m}(\phi)$.

Our first result gives a concrete bound on the average rank of the quadratic twists A_d. To state the result cleanly, we define the *absolute log-Selmer ratio* $t(\phi_d) = |\mathrm{ord}_3\, c(\phi_d)|$.

Theorem 5.2. Suppose A has dimension g and satisfies Assumption 2.2. Let $\Sigma \subset F^\times/F^{\times 2}$ be a subset defined by finitely many local conditions. Then the average Mordell–Weil rank of the quadratic twists A_d, for $d \in \Sigma$, is at most $g \cdot \mathrm{avg}_\Sigma \left(t(\phi_d) + 3^{-t(\phi_d)} \right)$. □

Proof. Note that $A_d(F)$ is a finitely generated $\mathcal{O}$-module, and that $A_d(F)$ has no 3-torsion for all but finitely many d. For such d, the rank of $A_d(F)$ is equal to $(g/k) \cdot \mathrm{rk}_{\mathcal{O}/\epsilon}\left(A_d(F)/\epsilon A_d(F)\right)$. Recall that k is the order of the ideal class of I in $\mathrm{Pic}(\mathcal{O})$, and ϵ is the generator of the kth power of the kernel ideal I of ϕ. We have $A_d(F)/\epsilon A_d(F) \subset \mathrm{Sel}_\epsilon(A_d)$, so it is enough to show that the average $\mathcal{O}/\epsilon$-module rank of $\mathrm{Sel}_\epsilon(A_d)$ is at most $k \cdot \mathrm{avg}_d \left(t(\phi_d) + 3^{-t(\phi_d)} \right)$. Since $\epsilon = \pi_k \pi_{k-1} \cdots \pi_2 \pi_1$, and since $\mathrm{Sel}_{\pi_i}(A_i) \simeq \mathrm{Sel}_\pi(A)$ for all i (Corollary 4.1), the rank of $\mathrm{Sel}_\epsilon(A_d)$ as an $\mathcal{O}/\epsilon$-module is at most $k \dim_{\mathbb{F}_3} \mathrm{Sel}_\pi(A)$. So it is enough to show that the average size of $\dim_{\mathbb{F}_3} \mathrm{Sel}_\pi(A_d)$ is at most $\mathrm{avg}_d \left(t(\phi_d) + 3^{-t(\phi_d)} \right)$.

To prove this, we fix $m \in \mathbb{Z}$ and show that the average $\mathbb{F}_3$-rank of $\mathrm{Sel}_\pi(A_d)$ for $d \in T_m(\phi)$ is at most $|m| + 3^{-|m|}$. We will suppose $m \geq 0$; the proof in the case $m < 0$ is similar. Then by Theorem 5.1, the average size of $\mathrm{Sel}_\phi(A_d)$ for $d \in T_m(\phi)$ is $1 + 3^m$. For any $r \in \mathbb{Z}$, we have the inequality $2r + 1 - 2m \leq 3^{r-m}$, so it follows that the average $\mathbb{F}_3$-rank of $\mathrm{Sel}_\phi(A_d)$ for $d \in T_m(\phi)$ is at most $m + \frac{1}{2}3^{-m}$. By Corollary 3.11, the average size of $\mathrm{Sel}_{\phi'}(B_d)$ for $d \in T_m(\phi)$ is $1 + 3^{-m}$, so the average $\mathbb{F}_3$-rank of $\mathrm{Sel}_{\phi'}(B_d)$ is at most $\frac{1}{2}3^{-m}$.

Using the exact sequence from (4.1),

$$\mathrm{Sel}_{\phi_d}(A_d) \to \mathrm{Sel}_\pi(A_d) \to \mathrm{Sel}_{\phi'_d}(B_d), \tag{5.1}$$

we deduce that the average $\mathbb{F}_3$-rank of $\mathrm{Sel}_\pi(A_d)$ is bounded by $m + 3^{-m}$, as desired. ■

Taking Σ to be $F^\times/F^{\times 2}$ in Theorem 5.2 gives Theorem 1.4. To show that a positive proportion of quadratic twists A_d have π-Selmer ranks 0 (resp. 1), we will need the following proposition.

Proposition 5.3. The sets $T_0(\phi)$ and $T_{\pm 1}(\phi)$ have positive density in $F^\times/F^{\times 2}$. □

Proof. We will prove the theorem for $T_0(\phi)$; the proof for $T_{\pm 1}(\phi)$ is similar. We need to construct a set $\Sigma \subset F^\times/F^{\times 2}$, defined by finitely many local conditions, such that $c(\phi_d) = 1$ for all $d \in \Sigma$. In fact, we construct Σ such that $c_\mathfrak{p}(\phi_d) = 1$, for all $\mathfrak{p} \nmid 3\infty$, and for all $d \in \Sigma$.

Let N_A be the conductor ideal of A. Then $\mathfrak{p}$ divides N_A if and only if A has bad reduction at $\mathfrak{p}$, and $c_\mathfrak{p}(\phi_d) = c_\mathfrak{p}(\phi'_d) = 1$ for all primes $\mathfrak{p}$ not dividing $6N_A\infty$, and for all d, by [Bhargava et al., Thm. 5.2]. To handle primes $\mathfrak{p}$ dividing $6N_A$, first note that there is exactly one squareclass $d \in F_\mathfrak{p}^\times/F_\mathfrak{p}^{\times 2}$ such that the denominator in (3.1), for $\phi = \phi_d$, is not equal to 1. Since there are at least four squareclasses in $F_\mathfrak{p}^\times$, we may choose a set $\tilde{\Sigma} \subset F^\times/F^{\times 2}$, defined by finitely many congruence conditions, such that both $c_\mathfrak{p}(\phi_d)$ and $c_\mathfrak{p}(\phi'_d)$ are integers, for all finite primes $\mathfrak{p}$ and all $d \in \tilde{\Sigma}$.

This already implies that $c_\mathfrak{p}(\phi_d) = 1 = c_\mathfrak{p}(\phi'_d)$ for all finite primes $\mathfrak{p} \nmid 3$ and all $d \in \tilde{\Sigma}$. Indeed, for such $\mathfrak{p}$ and d, we have $c_\mathfrak{p}(\pi_i) = c_\mathfrak{p}(\pi) = c_\mathfrak{p}(\phi_d) c_\mathfrak{p}(\phi'_d)$, so that the ratios $c_\mathfrak{p}(\pi_i)$ are integers whose product is 1:

$$c_\mathfrak{p}(\pi_1) c_\mathfrak{p}(\pi_2) \cdots c_\mathfrak{p}(\pi_k) = c_\mathfrak{p}(\epsilon) = c_\mathfrak{p}(A_d)/c_\mathfrak{p}(A_d) = 1.$$

Here we have used Proposition 3.1. It follows that both $c_\mathfrak{p}(\phi_d)$ and $c_\mathfrak{p}(\phi'_d)$ are positive integers whose product is 1, and hence both of these local Selmer ratios are 1, as claimed.

For the computation at primes $\mathfrak{p} \mid 3$, we abbreviate $\gamma_{\pi_i} = \gamma_{\pi_i, F_\mathfrak{p}}$ and $\gamma_\epsilon = \gamma_{\epsilon, F_\mathfrak{p}}$. Then

$$\prod_{i=1}^{k} c_\mathfrak{p}(\pi_i) = \prod_{i=1}^{k} \gamma_{\pi_i} = \gamma_\epsilon = 3^{k[F_\mathfrak{p} : \mathbb{Q}_3]},$$

for all d, by Proposition 3.1, Lemma 3.6, and Lemma 3.7. Since $c_{\mathfrak{p}}(\pi_i) = c_{\mathfrak{p}}(\pi)$, we have that $c_{\mathfrak{p}}(\pi) = c_{\mathfrak{p}}(\phi_d)c_{\mathfrak{p}}(\phi'_d) = 3^{[F_{\mathfrak{p}}\colon \mathbb{Q}_3]}$. Writing

$$c_3(\phi_d) := \prod_{\mathfrak{p}|3} c_{\mathfrak{p}}(\phi_d) \quad \text{and} \quad c_3(\phi'_d) := \prod_{\mathfrak{p}|3} c_{\mathfrak{p}}(\phi'_d),$$

we conclude that for $d \in \tilde{\Sigma}$, the product $c(\pi) = c_3(\phi_d)c_3(\phi'_d)$ is a power of 3 satisfying

$$1 \leq c_3(\phi_d)c_3(\phi'_d) \leq 3^{[F\colon \mathbb{Q}]}.$$

In particular, $1 \leq c_3(\phi_d) \leq 3^{[F\colon \mathbb{Q}]}$ for all $d \in \tilde{\Sigma}$.

Finally, if $\mathfrak{p}$ is a (real) archimedean place of F, then $c_{\mathfrak{p}}(\phi_d)$ is equal to $1/3$ or 1, depending on whether or not $A[\phi_d](F_{\mathfrak{p}})$ is non-trivial. Thus, we can impose sign conditions on d so that the archimedean contribution $c_\infty(\phi_d) := \prod_{\mathfrak{p}|\infty} c_{\mathfrak{p}}(\phi_d)$ is equal to 3^{-n} for any n satisfying $1 \leq n \leq [F\colon \mathbb{Q}]$.

It follows from the above discussion that the subset $\Sigma \subset \tilde{\Sigma}$ defined by

$$\Sigma = \left\{ d \in \tilde{\Sigma}\colon c_3(\phi_d)c_\infty(\phi_d) = 1 \right\},$$

has positive density in $F^\times/F^{\times 2}$. Moreover, $c(\phi_d) = 1$ for all $d \in \Sigma$, as desired. ■

Theorem 5.4. A proportion of at least $\frac{1}{2}\mu(T_0(\phi))$ of the quadratic twists A_d have rank 0. □

Proof. The map $\epsilon\colon A_d \to A_d$ is an isogeny and $A_d(F)/\epsilon A_d(F) \subset \mathrm{Sel}_\epsilon(A_d)$. Thus, if $\mathrm{Sel}_\epsilon(A_d) = 0$, then $A_d(F)$ has rank 0. So it is enough to show that at least $\frac{1}{2}\mu(T_0(\phi))$ of twists satisfy $\mathrm{Sel}_\epsilon(A_d) = 0$. Since $\mathrm{Sel}_{\pi_i}(A_i) \simeq \mathrm{Sel}_\pi(A)$, and $\epsilon = \pi_k \cdots \pi_1$, it is enough to prove that at least $\frac{1}{2}\mu(T_0(\phi))$ of twists satisfy $\mathrm{Sel}_\pi(A_d) = 0$.

By Theorem 5.1, the average size of $\mathrm{Sel}_\phi(A_d)$ for $d \in T_0(\phi)$ is 2. Since $\mathrm{Sel}_\phi(A_d)$ is an $\mathbb{F}_3$-vector space, it follows that at least 50% of d in $T_0(\phi)$ are such that $\mathrm{Sel}_\phi(A_d) = 0$. By Theorem 4.2, 100% of these d satisfy $\mathrm{Sel}_{\phi'_d}(A_d) = 0$, as well. From the exact sequence (5.1) we see that $\mathrm{Sel}_\pi(A_d) = 0$ for all such d, proving the theorem. ■

In the case where A admits an $\mathcal{O}$-linear polarization of degree prime to 3, Theorem 1.1 follows immediately from Proposition 5.3 and Theorem 5.4. The general case follows from this one using Zarhin's trick, i.e. that $(A \times \hat{A})^4$ is principally polarized. To run this argument, one must allow abelian varieties with RM by a totally real étale $\mathbb{Q}$-algebra which is not necessarily a field, but this does not change the proofs in Section 2.

To prove Theorem 1.3 we will need the following result.

Theorem 5.5. A proportion of at least $\frac{5}{6}\mu(T_{\pm 1}(\phi))$ of the twists A_d satisfy $\dim_{\mathbb{F}_3} \mathrm{Sel}_\pi(A_d) = 1$. □

Proof. We first consider $T_1(\phi)$. As before, we may assume this set has positive density. By Theorem 5.1, the average size of $\#\mathrm{Sel}_\phi(A_d)$ on $T_1(\phi)$ is 4. On the other hand, by Theorem 4.2, the $\mathbb{F}_3$-dimension of $\mathrm{Sel}_\phi(A_d)$ is at least 1 for 100% of twists $d \in T_1(\phi)$. It follows that for at least $\frac{5}{6}$ of such d, we have $\#\mathrm{Sel}_\phi(A_d) = 3$ and (by Theorem 4.2) that $\#\mathrm{Sel}_{\phi'}(B_d) = 1$. By the exactness of (5.1), we conclude that $\dim_{\mathbb{F}_3} \mathrm{Sel}_\pi(A_d) = 1$ for such d.

Next we consider $T_{-1}(\phi)$. By [Bhargava et al., Thm. 1.1], the average size of $\mathrm{Sel}_\phi(A_d)$ for $d \in T_{-1}(\phi)$ is $\frac{4}{3}$. It follows that at least $\frac{5}{6}$ of $d \in T_{-1}(\phi)$ satisfy $\#\mathrm{Sel}_\phi(A_d) = 1$ and (by Theorem 4.2) that $\#\mathrm{Sel}_{\phi'}(B_d) = 3$. For such d, the $\mathbb{F}_3$-dimension of $\mathrm{Sel}_\pi(A_d)$ is either 0 or 1. But by Theorem 4.4, the $\mathbb{F}_3$-dimension of $\mathrm{Sel}_\pi(A_d)$ is odd, so $\mathrm{Sel}_\pi(A_d)$ has $\mathbb{F}_3$-rank 1 for at least $\frac{5}{6}$ of d in $T_{-1}(\phi)$. ■

Proof of Theorem 1.3. The first part of Theorem 1.3 follows immediately from Proposition 5.3 and Theorem 5.5. For the second part, first note that there are isomorphisms

$$C_d(F)/\pi A_d(F) \simeq A_{i+1,d}(F)/\pi_i A_{i,d}(F)$$

for all $1 \leq i \leq k$ and all $d \in F^\times/F^{\times 2}$, by Proposition 2.9. Thus, if $A_d(F)$ has no 3-torsion (which is true for almost all d) and has rank ng, then $A_d(F)/\epsilon A_d(F)$ has rank n over $\mathcal{O}/\epsilon$ and $C_d(F)/\pi A_d(F)$ has $\mathbb{F}_3$-dimension n. We also have the short exact sequence

$$0 \to C_d(F)/\pi A_d(F) \to \mathrm{Sel}_\pi(A_d) \to Ш(A_d)[\pi] \to 0.$$

Thus, if $\dim_{\mathbb{F}_3} \mathrm{Sel}_\pi(A_d) = 1$, then either A_d has rank g or $\dim_{\mathbb{F}_3} Ш(A_d)[\pi] = 1$. But if $Ш(A_d)$ is finite, then $Ш(A_d)[\pi]$ has square order [Li, 2017, Thm. 3.3], so the latter case cannot occur. ■

6 Optimal quotients of prime level

In this section we prove Theorem 1.5. First we will verify that Theorem 1.1 is applicable; for this we use Mazur's study of the Eisenstein ideal to prove that the relevant kernel ideal is invertible. Then we compute various local Selmer ratios, in order to calculate the explicit bounds given in the Theorem. We first set notation and terminology.

Fix a prime p and let $\mathbb{T}$ be the $\mathbb{Z}$-algebra of Hecke operators acting on the space of weight 2 cuspforms on $\Gamma_0(p)$. If f is a newform for $\Gamma_0(p)$, then there is an induced homomorphism $\mathbb{T} \to \mathbb{C}$ giving the action of Hecke operators on f. Let I_f denote the kernel of this homomorphism. Then $A = J_0(p)/I_f J_0(p)$ is an abelian variety over $\mathbb{Q}$ and is called the *optimal quotient* corresponding to f. The endomorphism algebra $\mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q}$ is isomorphic to $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$, where $\mathcal{O} := \mathbb{T}/I_f$. Mazur proved [Mazur, 1977, Prop. II.9.5] that $\mathbb{T} = \mathrm{End}_{\mathbb{Q}}(J_0(p))$, from which it follows that $\mathbb{T}/I_f$ is a subring of $\mathrm{End}_{\mathbb{Q}}(A)$ of finite index, though not necessarily equal to $\mathrm{End}_{\mathbb{Q}}(A)$. In any case, A has RM by $\mathcal{O}$.

If $p \equiv 1 \pmod 9$, then there is at least one optimal quotient A with a rational point of order 3. If moreover $p \not\equiv 1 \pmod{27}$, then there is exactly one such quotient, corresponding to a single Galois orbit of newforms, and this A has a unique subgroup of order 3, which is the image of a rational cuspidal subgroup of order 3 in $J_0(p)$. These facts follow from [Emerton, 2003, Thm. B].

Let A be this unique optimal quotient, $P \in A(\mathbb{Q})$ a point of order 3, and $B = A/\langle P \rangle$ the quotient. By [Emerton, 2003, Thm. 4.13], the ring $\mathcal{O}$ necessarily contains an ideal I of index 3 such that P is contained in $A[I]$. Specifically, if $\mathfrak{I} \subset \mathbb{T}$ is the Eisenstein ideal, then I is the image of $(3, \mathfrak{I})$ under the map $\mathbb{T} \to \mathbb{T}/I_f$. By Remark 2.1, the quotient $\phi\colon A \to B$ is an $\mathcal{O}$-linear 3-isogeny with kernel ideal I. Since we work over $\mathbb{Q}$, every polarization of A is $\mathcal{O}$-linear as well.

Proposition 6.1. The kernel ideal I is an invertible $\mathcal{O}$-module. □

Proof. It is enough to check that I is a locally free $\mathcal{O}$-module, i.e. that $I_{\mathfrak{p}} \simeq \mathcal{O}_{\mathfrak{p}}$ as $\mathcal{O}_{\mathfrak{p}}$-modules, for all primes $\mathfrak{p}$ of $\mathcal{O}$. Since I has index 3 in $\mathcal{O}$, it is itself a prime ideal, and $I_I \simeq \mathcal{O}_I$ as $\mathcal{O}_I$-modules by Mazur's principality theorem [Mazur, 1977, Thm. II.18.10 and 19.1]. Here it is crucial that $p \not\equiv 1 \pmod{27}$, so that the image of $(3, \mathfrak{I})$ in $\mathcal{O}$ is all of I, and not some smaller ideal. On the other hand, if $\mathfrak{p} \neq I$, then the inclusion $I \hookrightarrow \mathcal{O}$ induces an isomorphism $I_{\mathfrak{p}} \simeq \mathcal{O}_{\mathfrak{p}}$. ■

Corollary 6.2. The abelian variety A and the isogeny ϕ satisfy the hypotheses of Theorem 1.1. □

It follows that a positive proportion of twists A_d have rank 0 and that the average rank of $A_d(\mathbb{Q})$ is bounded. To say something more quantitative, we need to compute various local Selmer ratios.

6.1 Selmer ratios for ϕ_d

In this section, d will always be a squarefree integer. For each d, let $\phi_d\colon A_d \to B_d$ be the d-th twist of the 3-isogeny $\phi\colon A \to B$. The following four propositions compute the local Selmer ratios $c_\ell(\phi_d)$ for all primes $\ell \leq \infty$ and all d.

Proposition 6.3. If $\ell \notin \{3, p, \infty\}$, then $c_\ell(\phi_d) = 1$, for all d. □

Proof. This is [Bhargava et al., Thm. 6.2]. ■

Proposition 6.4. If $\ell = \infty$, we have

$$c_\infty(\phi_d) = \begin{cases} 1/3 & d > 0 \\ 1 & d < 0. \end{cases}$$

□

Proof. We have $c_\infty(\phi_d) = \#\ker(\phi_d)(\mathbb{R})^{-1}$ and $\#\ker(\phi)(\mathbb{R}) = \#\langle P \rangle = 3$. ■

Proposition 6.5. If $\ell = 3$, then $c_3(\phi_d) = 1$ for all d. □

Proof. Since A_d has a quadratic twist of good reduction, we have $c_3(A_d) = c_3(B_d)$ for all d. For elliptic curves this was proven in [Bhargava et al., Lem. 11.1], but the proof holds equally well for higher dimensional abelian varieties. Thus, we have

$$c_3(\phi_d) = \gamma_{\phi,\mathbb{Q}_3} \frac{c_3(B_d)}{c_3(A_d)} = \gamma_{\phi,\mathbb{Q}_3} = 1,$$

the final equality since ϕ extends to an étale isogeny of Néron models over $\mathbb{Z}_3$ by [Mazur, 1977, II.11.11]. ∎

The remaining case $\ell = p$ is handled by the following proposition.

Proposition 6.6. If $d \in \mathbb{Z}$ is squarefree then

$$c_p(\phi_d) = \begin{cases} 1/3 & d \in \mathbb{Z}_p^{\times 2} \\ 1 & \text{otherwise.} \end{cases}$$

□

Proof. [‡] For this proof, we consider A_d and B_d as abelian varieties over $\mathbb{Q}_p$, and write A_d^{an} and B_d^{an} for their rigid-analytifications. First we consider the case $d \in \mathbb{Z}_p^{\times 2}$. In this case, $A_d \simeq A$ and $B_d \simeq B$ both have (purely) toric reduction over $\mathbb{Q}_p$. Moreover, since A is an Eisenstein quotient, they have *split* toric reduction. We may therefore write $A^{\mathrm{an}} = T/\Lambda$, where $T = \mathbb{G}_{m,\mathbb{Q}_p}^{\mathrm{an},g}$ is a split analytic torus of rank $g = \dim A$, and Λ is a full rank lattice defined over $\mathbb{Q}_p$. Set $\Lambda^\vee = \mathrm{Hom}(T, \mathbb{G}_{m,\mathbb{Q}_p}^{\mathrm{an}})$.

The local Selmer ratio $c_p(\phi)$ is equal to the ratio $c_p(B)/c_p(A)$ of Tamagawa numbers. By definition $c_p(A) = \#\Phi(\mathbb{F}_p)$, where $\Phi = \Phi_A$ is the component group of the special fiber of the Néron model $\mathscr{A}$ of A. Since A has split toric reduction, the étale group scheme Φ is constant over $\mathbb{F}_p$, so we may regard it as a group. Grothendieck's monodromy pairing leads to the following exact sequence

$$0 \to \Lambda \to \mathrm{Hom}(\Lambda^\vee, \mathbb{Z}) \to \Phi \to 0.$$

This gives an explicit way to compute the specialization homomorphism $A(\mathbb{Q}_p) \to \Phi$. Namely, if $x \in A(\mathbb{Q}_p)$, let $t \in T(\mathbb{Q}_p)$ be any lift of x, and let $\tilde{t} \in \mathrm{Hom}(\Lambda^\vee, \mathbb{Z})$ be the homomorphism:

$$\tilde{t} \colon f \mapsto \mathrm{val}(f(t)).$$

Then the image of x in Φ under specialization is the image of $\tilde{t}$ under the quotient $\mathrm{Hom}(\Lambda^\vee, \mathbb{Z}) \to \Phi$.

By [Emerton, 2003, Thm. B], the specialization map induces an isomorphism $A_{\mathrm{tors}}(\mathbb{Q}) \simeq \Phi$. In particular, we deduce that the order 3 point P does not lie in the subgroup $\mu_3^g \subset T(\mathbb{Q}_p)$ of $A(\mathbb{Q}_p)[3]$. It follows that we may choose lattice generators $\Lambda = \langle q_1, \dots, q_g \rangle$ such that $P = \bar{q}_0$, where $q_0 \in T$ is a cube root of q_1 and $\bar{q}_0$ denotes the image of q_0 in $A(\mathbb{Q}_p)$. Therefore $B = T/\Lambda_B$, where $\Lambda_B = \langle q_0, q_2, \dots, q_g \rangle$. In particular, we have $\Lambda_B^\vee = \Lambda^\vee$ and the monodromy sequence for B reads:

$$0 \to \Lambda_B \to \mathrm{Hom}(\Lambda^\vee, \mathbb{Z}) \to \Phi_B \to 0.$$

We deduce that $\Phi = \Phi_A$ surjects onto Φ_B with kernel of order 3; hence $c_p(\phi) = c_p(B)/c_p(A) = 1/3$.

Finally, we consider non-square $d \in \mathbb{Q}_p^\times$. Let $K = \mathbb{Q}_p(\sqrt{d})$, and let ϕ_K be the base change of the isogeny ϕ to K. Since $p > 3$, we have the general formula (see [Dokchitser and Dokchitser, 2015, Lem. 4.6])

$$c_p(\phi_K) = c_p(\phi_d) c_p(\phi).$$

But the computation above also gives $c_p(\phi_K) = 1/3$. We conclude that $c_p(\phi_d) = 1$. ∎

Putting together Propositions 6.3-6.6, we can compute the global Selmer ratio $c(\phi_d) = \prod_{p \le \infty} c_p(\phi_d)$ for any squarefree d. In particular, we can determine the sets

$$T_m(\phi) = \left\{ d \in F^\times / F^{\times 2} \colon c(\phi_d) = 3^m \right\}$$

defined in the previous section, and their densities $\mu(T_m(\phi))$ within $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. We find:

Corollary 6.7. For the isogeny $\phi \colon A \to B$, we have

$$\mu(T_m(\phi)) = \begin{cases} \frac{1}{2} - \frac{1}{4}\frac{p}{p+1} & m = 0 \\ \frac{1}{2} & m = -1 \\ \frac{1}{4}\frac{p}{p+1} & m = -2 \\ 0 & \text{else.} \end{cases}$$

□

[‡] This proof relies on the p-adic uniformization of abelian varieties; we refer the reader to Papikian [2013] for background.

Proof. For example, for $m = -2$, we need $d > 0$ and $d \in \mathbb{Z}_p^{\times 2}$. This gives a density of

$$\frac{1}{2} \cdot \frac{\frac{1}{2}p(p-1)}{p^2-1} = \frac{1}{4}\frac{p}{p+1}$$

of all square classes. The computations for other m are similar; alternatively, they can be deduced from pure thought. Indeed, $\mu(T_m(\phi)) = 0$ for $m \notin \{-2, -1, 0\}$, so parity ensures $T_{-1}(\phi) = \frac{1}{2}$. Since the densities must add to 1, we deduce $\mu(T_0)(\phi) = \frac{1}{2} - \frac{1}{4}\frac{p}{p+1}$ as well. ■

It follows from the results in Section 5 that the average $\mathcal{O}$-rank of A_d is at most 13/9 and that at least 1/8 of twists have rank 0. Note that this is not as strong as what is claimed in Theorem 1.5! This is because there is another 3-isogeny $\psi\colon A \to B'$, which we will use to deduce even better rank bounds in the next subsection.

6.2 Selmer ratios for ψ_d

First we must define B' and the isogeny $\psi\colon A \to B'$. Let $\Sigma \subset J_0$ be the Shimura subgroup of J_0, thought of, for the moment, as schemes over $\operatorname{Spec}\mathbb{Z}$. Then Σ is a finite μ-type group of order equal to the numerator of $(p-1)/12$; see [Mazur, 1977, §II.11] for its definition. We let Σ_3 be the 3-primary subgroup of Σ. Since $p \equiv 10$ or 19 (mod 27), Σ_3 has order 3.

Lemma 6.8. The image of Σ_3 under the map $J_0(p) \to A$ is a rational subgroup of order 3. □

Proof. Specialization induces an isomorphism $\Sigma(\mathbb{F}_p) \to \Phi_{J_0(p)}$ onto the component group over $\mathbb{F}_p$ [Mazur, 1977, Prop. II.11.9]. Since this is compatible with the surjection $\Phi_{J_0(p)} \to \Phi_A$, it follows (using [Emerton, 2003, Thm. B]) that the image of Σ_3 in A is a subgroup of order 3. ■

We let $\psi\colon A \to B'$ be the 3-isogeny of abelian varieties over $\mathbb{Q}$ whose kernel is the image of Σ_3.

Corollary 6.9. The 3-isogeny $\psi\colon A \to B'$ satisfies the hypotheses of Theorem 1.1. □

Proof. Since Σ_3 is Eisenstein [Mazur, 1977, II.11.7], we have $\ker\psi \subset A[I]$, where recall I is the kernel ideal of ϕ, which we have already identified as the image of the 3-part of the Eisenstein ideal. This gives a decomposition $A[I] = \langle P\rangle \oplus \ker\psi$ as $\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-modules. It also means that I is the kernel ideal of ψ, and by Proposition 6.1, the hypotheses of Theorem 1.1 hold. ■

The next several propositions compute the local Selmer ratios $c_\ell(\psi_d)$ for all primes ℓ and all squarefree $d \in \mathbb{Z}$. The proof of the first proposition is as in the previous subsection.

Proposition 6.10. If $\ell \notin \{3, p, \infty\}$, then $c_\ell(\psi_d) = 1$, for all d. □

Proposition 6.11. If $\ell = \infty$, we have

$$c_\infty(\psi_d) = \begin{cases} 1 & d > 0 \\ 1/3 & d < 0. \end{cases}$$

□

Proof. This is because $\ker\psi \simeq \Sigma_3 \simeq \mu_3$ as group schemes over $\mathbb{R}$. ■

Proposition 6.12. If $\ell = 3$, then $c_3(\psi_d) = 3$ for all d. □

Proof. As in the previous subsection, we have $c_3(A_d) = c_3(B_d)$ for all d. Let $\pi\colon A \to A/A[I]$ be the canonical $(3,3)$-isogeny. Also let $\tilde{\phi}\colon B' \to A/A[I]$ be the unique 3-isogeny such that $\tilde{\phi}\psi = \pi$. Then $\tilde{\phi}$ is étale over $\mathbb{Z}_3$ since ϕ is, and so $c_3(\tilde{\phi}) = 1$. By Lemmas 3.4, 3.7, and 3.9, we compute that

$$c_3(\psi) = c_3(\pi)c_3(\tilde{\phi})^{-1} = c_3(\pi) = 3.$$

■

Proposition 6.13. If $d \in \mathbb{Z}$ is squarefree then

$$c_p(\psi_d) = \begin{cases} 1/3 & d \in \mathbb{Z}_p^{\times 2} \\ 1 & \text{otherwise.} \end{cases}$$

□

Proof. Since $\mu_3 \subset \mathbb{Q}_p^\times$, the generator of $\ker \psi$ is defined over $\mathbb{Q}_p$. Since this generator maps to a non-trivial element of the component group Φ_A, we may proceed exactly as in Proposition 6.6. ∎

Putting together Propositions 6.10-6.13, we deduce:

Corollary 6.14. For the isogeny $\psi\colon A \to B'$, we have

$$\mu(T_m(\psi)) = \begin{cases} \frac{1}{2} - \frac{1}{4}\frac{p}{p+1} & m = 1 \\ \frac{1}{2} & m = 0 \\ \frac{1}{4}\frac{p}{p+1} & m = -1 \\ 0 & \text{else.} \end{cases}$$

□

Proof of Theorem 1.5. To prove parts *a*) through *c*), we use the densities computed in Corollary 6.14. Part *a*) follows from Theorem 5.2, part *b*) follows from Theorem 5.4, and part *c*) follows from Theorem 5.5. This is also shows that at least 5/12 of twists A_d have $\mathcal{O}$-rank 1, if we further assume that $Ш(A_d)[3^\infty]$ is finite for all d.

Part *d*) will follow from comparing Propositions 6.3-6.6 to Propositions 6.10-6.13. The key observation is that

$$T_{-2}(\phi) \subset T_0(\psi).$$

It follows that for $d \in T_{-2}(\phi)$, the average $\mathcal{O}$-rank of A_d is 1, due to our average rank bound for $d \in T_0(\psi)$. Since the parity of $\dim_{\mathbb{F}_3} \mathrm{Sel}_\pi(A_d)$ is even for $d \in T_0(\psi)$, by Theorem 4.4, we deduce that for at least 50% of such d, both A_d and B_d have rank 0. On the other hand, for $d \in T_{-2}(\phi)$, and $d \neq 1$, we have $\dim_{\mathbb{F}_3} \mathrm{Sel}_{\phi'_d}(B_d) \geq 2$ by Theorem 4.2. Here, $\phi'\colon B \to C$ is the isogeny such that $\phi'\phi = \pi$. It follows that $\#Ш(B_d)[3] \geq 9$ for almost all $d \in T_{-2}(\phi)$ such that B_d has rank 0. The density of this set of twists is at least $\frac{1}{2}\mu(T_{-2}(\phi)) = \frac{1}{8}\frac{p}{p+1}$, which proves part *d*). ∎

7 Examples

We give explicit examples of abelian varieties of dimension $g > 1$ over $\mathbb{Q}$ satisfying the hypotheses of Theorems 1.1 and 1.3, and Corollary 1.7.

The first few examples were found by searching through rational points on explicit models of Hilbert modular surfaces. These are moduli spaces of principally polarized abelian surfaces with real multiplication by a fixed order $\mathcal{O}$ in a real quadratic number field K. For our purposes, we restrict to those K with an ideal of index 3. If we take $K = \mathbb{Q}(\sqrt{3p})$ with p equal to 1, 2, or any prime $p \equiv 3 \pmod 4$, then we can take the ideal to be principal as well. In those cases, we have $3\mathcal{O}_K = \pi^2\mathcal{O}_K$ for some element $\pi \in \mathcal{O}_K$ of norm ± 3. It follows that if $A/\mathbb{Q}$ has RM by $\mathcal{O}_K$, then $A(\mathbb{Q})$ has a non-trivial π-torsion point if and only if $A(\mathbb{Q})$ has a point of order 3.

To find examples of such A, we simply searched through the tables of genus two curves in Elkies and Kumar [2014], while checking in Magma for a rational point of order 3 on the Jacobian.

Example 7.1. The Jacobian J of the genus two curve

$$C\colon y^2 = x^5 - x^4 + x^3 - 3x^2 - x + 5$$

has RM by $\mathbb{Z}[\sqrt{3}]$ over $\mathbb{Q}$ and a non-trivial $\sqrt{3}$-torsion point in $J(\mathbb{Q})$. Thus Theorems 1.1 and 1.3 apply. As C is hyperelliptic, Corollary 1.7 applies as well, and shows that for a positive proportion of twists d, we have $C_d(\mathbb{Q}) = \{\infty, (-1, 0)\}$. □

Example 7.2. The Jacobian J of the genus two curve

$$C\colon y^2 = -72x^6 + 84x^5 + 127x^4 - 123x^3 - 83x^2 + 51x + 25$$

has RM by $\mathbb{Z}[\sqrt{6}]$ over $\mathbb{Q}$ and a non-trivial $(3 + \sqrt{6})$-torsion point P in $J(\mathbb{Q})$. In this case, we have $B = J/\langle P\rangle$, which is itself principally polarized (see Remark 2.2) and hence a Jacobian of some genus 2 curve C'. If one could write down a model for C', then the bound on the average rank of J_d given in Theorem 5.2 could be computed explicitly, and our lower bounds on the proportion of twists having rank 0 (resp. π-Selmer rank 1) could be made explicit as well. □

We found the following example in the LMFDB LMFDB Collaboration [2013].

Example 7.3. The Jacobian J of the genus two curve

$$C\colon y^2 + (x^3 + 1)y = x^5 + 4x^4 + 6x^3 + 10x^2 + 3x + 1$$

has RM by $\mathbb{Z}[\sqrt{3}]$ over $\mathbb{Q}$ and a non-trivial $\sqrt{3}$-torsion point in $J(\mathbb{Q})$. This J seems to be isogenous to another Jacobian which is a quotient of $J_0(65)$, and which has appeared in the literature a few times already; see [González et al., 2005, §4.2] and [Li, 2017, Rem. 3.4]. □

Of course, Theorem 1.5 gives many examples in dimension $g \geq 2$, and with explicit bounds on the rank statistics. These A are optimal quotients of $J_0(p)$ with a point of order 3, and with $p \equiv 10$ or $19 \pmod{27}$. There are only two cases where A is an elliptic curve: these are at levels 19 and 37 (see [Mazur, 1977, III.7.5]).

Example 7.4. For p less than 1000, there are 4 examples of abelian surface quotients of $J_0(p)$ with a point of order 3 ($p = 73, 307, 487$, and 577); all of these have RM by $\mathbb{Q}(\sqrt{13})$. These surfaces need not be principally polarized in general, but they may be isogenous to a principally polarized abelian surface. For example, when $p = 73$, A seems to be isogenous to the Jacobian of the genus two curve

$$C\colon y^2 + (x^3 + x + 1)y = -x^6 - 8x^5 - 16x^4 + 25x^3 - 40x^2 + 31x - 8$$

If this can be verified, then the explicit version of Corollary 1.7 would imply that at least 25% of twists C_d have no rational points. □

The author guesses that Theorem 1.5 applies to only finitely many abelian surfaces, and to only finitely many abelian varieties of any given dimension g. The first example with $g > 2$ is:

Example 7.5. Let A be the 'minus part' of the modular Jacobian $J_0(127)$. This is a simple 7-dimensional abelian variety corresponding to the unique Galois orbit of newforms of level 127 with root number $+1$. In particular, it is the only Eisenstein optimal quotient of $J_0(127)$, hence has a torsion point of order 3. The modular degree of A is 8, and so A has a polarization of degree prime to 3. It follows from Theorem 1.5 that at least 25% of twists A_d have rank 0, and assuming $Ш(A_d)$ finite, at least 5/12 of twists have rank 7. □

In the next example, Theorem 1.5 does not apply since $p \equiv 1 \pmod{27}$, but we can verify the hypotheses of Theorem 1.1 nonetheless.

Example 7.6. There is a unique Eisenstein optimal quotient A of $J_0(109)$; it is 4-dimensional. We have $A(\mathbb{Q}) \simeq \mathbb{Z}/9\mathbb{Z}$ and $\mathrm{End}(A) \simeq \mathcal{O}_K$, for the quartic field K with minimal polynomial $x^4 - 5x^3 + 3x^2 + 6x + 1$. One checks that the order 3 subgroup G of $A(\mathbb{Q})$ is killed by the unique ideal I of index 3 in $\mathcal{O}_K$. It follows that $A \to A/G$ is $\mathcal{O}_K$-linear with invertible kernel ideal. The proof of Theorem 1.5 now applies to A and so we can conclude that the average $\mathcal{O}$-rank is at most 7/6 and at least 25% of twists have rank 0. Sage reports that the modular degree of A is 32, so A admits an $\mathcal{O}$-linear polarization of degree prime to 3. Thus, at least 5/12 of twists have $\mathcal{O}$-rank 1, assuming $Ш(A_d)$ is finite. □

Acknowledgements: The author thanks Manjul Bhargava, Pete Clark, Victor Flynn, Eyal Goren, Ben Howard, Zev Klagsbrun, Robert Lemke Oliver, Keerthi Madapusi Pera, Barry Mazur, Bjorn Poonen, Alice Silverberg, Drew Sutherland, and Yuri Zarhin for helpful conversations. We also thank the referees for helpful comments.

References

Jennifer S. Balakrishnan and Netan Dogra. An effective Chabauty-Kim theorem. *Compos. Math.*, 155(6): 1057–1075, 2019. ISSN 0010-437X. doi: 10.1112/s0010437x19007243. URL https://doi.org/10.1112/s0010437x19007243.

M. Bhargava, Z. Klagsbrun, R. J. Lemke Oliver, and A. Shnidman. Three-isogeny Selmer groups and ranks of abelian varieties in quadratic twist families over a number field. *Preprint available at http://arxiv.org/abs/1709.09790.*

Manjul Bhargava and Benedict H. Gross. The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point. In *Automorphic representations and L-functions*, volume 22 of *Tata Inst. Fundam. Res. Stud. Math.*, pages 23–91. Tata Inst. Fund. Res., Mumbai, 2013.

Manjul Bhargava and Arul Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Ann. of Math. (2)*, 181(2):587–621, 2015. ISSN 0003-486X. doi: 10.4007/annals.2015.181.2.4. URL http://dx.doi.org/10.4007/annals.2015.181.2.4.

Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang. A positive proportion of locally soluble hyperelliptic curves over $\mathbb{Q}$ have no point over any odd degree extension. *J. Amer. Math. Soc.*, 30(2):451–493, 2017. ISSN 0894-0347. doi: 10.1090/jams/863. URL http://dx.doi.org/10.1090/jams/863. With an appendix by Tim Dokchitser and Vladimir Dokchitser.

Manjul Bhargava, Zev Klagsbrun, Robert J. Lemke Oliver, and Ari Shnidman. Elements of given order in Tate-Shafarevich groups of abelian varieties in quadratic twist families. *arXiv e-prints*, art. arXiv:1904.00116, Mar 2019.

Daniel Bump, Solomon Friedberg, and Jeffrey Hoffstein. Nonvanishing theorems for L-functions of modular forms and their derivatives. *Invent. Math.*, 102(3):543–618, 1990. ISSN 0020-9910. URL https://doi.org/10.1007/BF01233440.

J. W. S. Cassels. Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer. *J. Reine Angew. Math.*, 217:180–199, 1965. ISSN 0075-4102. doi: 10.1515/crll.1965.217.180. URL http://dx.doi.org/10.1515/crll.1965.217.180.

Kkestutis Česnavičius. p-Selmer growth in extensions of degree p. *J. Lond. Math. Soc. (2)*, 95(3):833–852, 2017. ISSN 0024-6107. doi: 10.1112/jlms.12038. URL http://dx.doi.org/10.1112/jlms.12038.

Tim Dokchitser and Vladimir Dokchitser. Local invariants of isogenous elliptic curves. *Trans. Amer. Math. Soc.*, 367(6):4339–4358, 2015. ISSN 0002-9947. doi: 10.1090/S0002-9947-2014-06271-5. URL http://dx.doi.org/10.1090/S0002-9947-2014-06271-5.

Noam Elkies and Abhinav Kumar. K3 surfaces and equations for Hilbert modular surfaces. *Algebra Number Theory*, 8(10):2297–2411, 2014. ISSN 1937-0652. doi: 10.2140/ant.2014.8.2297. URL http://dx.doi.org/10.2140/ant.2014.8.2297.

Matthew Emerton. Optimal quotients of modular Jacobians. *Math. Ann.*, 327(3):429–458, 2003. ISSN 0025-5831. doi: 10.1007/s00208-003-0449-2. URL http://dx.doi.org/10.1007/s00208-003-0449-2.

Tom A. Fisher. The Cassels-Tate pairing and the Platonic solids. *J. Number Theory*, 98(1):105–155, 2003. ISSN 0022-314X. doi: 10.1016/S0022-314X(02)00038-0. URL http://dx.doi.org/10.1016/S0022-314X(02)00038-0.

Dorian Goldfeld. Conjectures on elliptic curves over quadratic fields. In *Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979)*, volume 751 of *Lecture Notes in Math.*, pages 108–118. Springer, Berlin, 1979.

Josep González, Jordi Guàrdia, and Victor Rotger. Abelian surfaces of GL_2-type as Jacobians of curves. *Acta Arith.*, 116(3):263–287, 2005. ISSN 0065-1036. doi: 10.4064/aa116-3-3. URL http://dx.doi.org/10.4064/aa116-3-3.

Andrew Granville. Rational and integral points on quadratic twists of a given hyperelliptic curve. *Int. Math. Res. Not. IMRN*, (8):Art. ID 027, 24, 2007. ISSN 1073-7928. URL https://doi.org/10.1093/imrn/rnm027.

Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986. ISSN 0020-9910. URL https://doi.org/10.1007/BF01388809.

Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. I. *Invent. Math.*, 178(3):485–504, 2009.

V. A. Kolyvagin and D. Yu. Logachëv. Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties. *Algebra i Analiz*, 1(5):171–196, 1989. ISSN 0234-0852.

Daniel Kriz and Chao Li. Goldfeld's conjecture and congruences between heegner points. *Forum Math. Sigma*, 7:e15, 2019. ISSN 2050-5094. doi: 10.1017/fms.2019.9. URL https://doi.org/10.1017/fms.2019.9.

Chao Li. Level raising mod 2 and obstruction to rank lowering. *International Mathematics Research Notices*, 2017.

The LMFDB Collaboration. The l-functions and modular forms database. http://www.lmfdb.org, 2013. [Online; accessed 16 September 2013].

B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186, 1977. ISSN 0073-8301. URL http://www.numdam.org/item?id=PMIHES_1977__47__33_0.

B. Mazur. On the arithmetic of special values of l-functions. *Invent. Math.*, (55):207–240, 1979.

J. S. Milne. *Arithmetic duality theorems*. BookSurge, LLC, Charleston, SC, second edition, 2006. ISBN 1-4196-4274-X.

D. Mumford. *Abelian Varieties*. Oxford University Press, first edition, 1970.

Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008. ISBN 978-3-540-37888-4. doi: 10.1007/978-3-540-37889-1. URL http://dx.doi.org/10.1007/978-3-540-37889-1.

Mihran Papikian. Non-Archimedean uniformization and monodromy pairing. In *Tropical and non-Archimedean geometry*, volume 605 of *Contemp. Math.*, pages 123–160. Amer. Math. Soc., Providence, RI, 2013. URL https://doi-org.proxy.bc.edu/10.1090/conm/605/12114.

Bjorn Poonen and Michael Stoll. The Cassels-Tate pairing on polarized abelian varieties. *Ann. of Math. (2)*, 150(3):1109–1149, 1999. ISSN 0003-486X. doi: 10.2307/121064. URL http://dx.doi.org/10.2307/121064.

Bjorn Poonen and Michael Stoll. Most odd degree hyperelliptic curves have only one rational point. *Ann. of Math. (2)*, 180(3):1137–1166, 2014. ISSN 0003-486X. doi: 10.4007/annals.2014.180.3.7. URL http://dx.doi.org/10.4007/annals.2014.180.3.7.

Kenneth A. Ribet. Abelian varieties over **Q** and modular forms. In *Algebra and topology 1992 (Taejŏn)*, pages 53–79. Korea Adv. Inst. Sci. Tech., Taejŏn, 1992.

Edward F. Schaefer. Class groups and Selmer groups. *J. Number Theory*, 56(1):79–114, 1996. ISSN 0022-314X. doi: 10.1006/jnth.1996.0006. URL http://dx.doi.org/10.1006/jnth.1996.0006.

Ananth N. Shankar. 2-Selmer groups of hyperelliptic curves with marked points. *Trans. Amer. Math. Soc.*, 372 (1):267–304, 2019. ISSN 0002-9947. doi: 10.1090/tran/7546. URL https://doi.org/10.1090/tran/7546.

V. Vatsal. Canonical periods and congruence formulae. *Duke Math. J.*, 98(2):397–419, 1999.

William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969. ISSN 0012-9593. URL http://www.numdam.org/item?id=ASENS_1969_4_2_4_521_0.