European Journal of Mathematics
https://doi.org/10.1007/s40879-022-00570-4

RESEARCH ARTICLE

Check for updates

Integral points on punctured abelian varieties

Samir Siksek[1]

Received: 28 April 2021 / Revised: 5 July 2022 / Accepted: 13 July 2022

Abstract
Let $A/\mathbb{Q}$ be an abelian variety such that $A(\mathbb{Q}) = \{0_A\}$. Let ℓ and p be rational primes, such that A has good reduction at p, and satisfying $\ell \equiv 1 \pmod{p}$ and $\ell \nmid \# A(\mathbb{F}_p)$. Let S be a finite set of rational primes. We show that $(A \setminus \{0_A\})(\mathcal{O}_{L,S}) = \varnothing$ for 100% of cyclic degree ℓ fields $L/\mathbb{Q}$, when ordered by conductor, or by absolute discriminant.

Keywords Abelian varieties · Cyclic fields · Integral points

Mathematics Subject Classification 11G10 · 11G0

1 Introduction

Let L be a number field and write $\mathcal{O}_L$ for its ring of integers. Let S be a finite set of places of L, and write $\mathcal{O}_{L,S}$ for the ring of S-integers in L. Let A be an abelian variety over L. A theorem of Faltings [6, Corollary 6.2] asserts that $(A \setminus D)(\mathcal{O}_{L,S})$ is finite for any ample divisor D of A (similar results are due to Silverman [21] and Vojta [27]). Write $0_A \in A$ for the origin. We refer to $A \setminus \{0_A\}$ as a punctured abelian variety, and refer to $(A \setminus \{0_A\})(\mathcal{O}_{L,S})$ as the set of S-integral points on $A \setminus \{0_A\}$. We recall that $(A \setminus \{0_A\})(\mathcal{O}_{L,S})$ is the set of points $P \in A(L)$ such that P does not reduce to 0_A modulo any $\mathfrak{P} \notin S$. If $\dim(A) = 1$, then the finiteness of $(A \setminus \{0_A\})(\mathcal{O}_{L,S})$ is a famous theorem of Siegel [22, Section IX.3]. Little is known about the integral points on $A \setminus \{0_A\}$ for $\dim(A) \geqslant 2$. A special case of the *Arithmetic Puncturing Problem* of Hassett and Tschinkel [10, Problem 2.13] asks whether the integral points on $A \setminus \{0_A\}$ are potentially dense. Integral points on punctured abelian varieties are considered in

Siksek is supported by the EPSRC grant *Moduli of Elliptic curves and Classical Diophantine Problems* (EP/S031537/1).

✉ Samir Siksek
s.siksek@warwick.ac.uk

[1] Mathematics Institute, University of Warwick, Coventry CV4 7AL, UK

Published online: 30 August 2022

[3, Section 8], [12] and [13]. The current paper explores an obstruction to the existence of S-integral points on $A \setminus \{0_A\}$.

For a finite prime $\mathfrak{P}$ of $\mathcal{O}_L$ we denote the residue field by $\mathbb{F}_{\mathfrak{P}} = \mathcal{O}_L/\mathfrak{P}$, and the completion of L at $\mathfrak{P}$ by $L_{\mathfrak{P}}$. If A has good reduction at $\mathfrak{P}$ we will write $A^1(L_{\mathfrak{P}})$ for the kernel of the reduction map $A(L_{\mathfrak{P}}) \to A(\mathbb{F}_{\mathfrak{P}})$.

Theorem 1.1 *Let K be a number field, and let A be an abelian variety defined over K satisfying $A(K) = \{0_A\}$. Let $\mathfrak{p}$ be a finite prime of $\mathcal{O}_K$ of good reduction for A. Let L/K be an extension of degree m. Suppose that*

(i) *$\mathfrak{p}$ is totally ramified in L;*
(ii) $\gcd(\# A(\mathbb{F}_{\mathfrak{p}}), m) = 1$.

Then $A(L) \subseteq A^1(L_{\mathfrak{P}})$ where $\mathfrak{P}$ be the unique prime of $\mathcal{O}_L$ above $\mathfrak{p}$. In particular, $(A \setminus \{0_A\})(\mathcal{O}_{L,S}) = \emptyset$, for any set of places S not containing $\mathfrak{P}$.

Remark Mazur and Rubin [15, Corollary 1.11] proved the existence, for any number field K, of elliptic curves E/K satisfying $E(K) = \{0_E\}$. By taking powers of such E we obtain abelian varieties A/K of any desired dimension satisfying $A(K) = \{0_A\}$.

Proof of Theorem 1.1 for L/K Galois The theorem is proved in Sect. 3. However, when L/K is Galois, the theorem admits a shorter and more conceptual proof, which we now give. Recall that the inertia subgroup $I_{\mathfrak{P}} \subseteq \mathrm{Gal}\,(L/K)$ is by definition the subset of $\sigma \in \mathrm{Gal}\,(L/K)$ such that $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}}$ for all $\alpha \in \mathcal{O}_L$. Since $\mathfrak{p}$ is totally ramified, we have $I_{\mathfrak{P}} = \mathrm{Gal}\,(L/K)$. We deduce that $\sigma(Q) \equiv Q \pmod{\mathfrak{P}}$ for all $Q \in A(L)$ and all $\sigma \in \mathrm{Gal}\,(L/K)$. Thus

$$\mathrm{Trace}_{L/K}(Q) = \sum_{\sigma \in \mathrm{Gal}\,(L/K)} \sigma(Q) \equiv mQ \pmod{\mathfrak{P}}.$$

However, $\mathrm{Trace}_{L/K}(Q) \in A(K) = \{0_A\}$ by assumption. Thus $mQ \equiv 0_A \pmod{\mathfrak{P}}$. Now, again as $\mathfrak{p}$ is totally ramified, $\mathbb{F}_{\mathfrak{P}} = \mathbb{F}_{\mathfrak{p}}$, and so $A(\mathbb{F}_{\mathfrak{P}}) = A(\mathbb{F}_{\mathfrak{p}})$. By assumption (ii) we have $Q \equiv 0_A \pmod{\mathfrak{P}}$ completing the proof. □

Remark The assumption that L/K is Galois is in fact merely needed to simplify the proof of the intermediate conclusion $\mathrm{Trace}_{L/K}(Q) \equiv mQ \pmod{\mathfrak{P}}$. Lemma 2.2 below shows that this intermediate conclusion holds without the Galois assumption.

Corollary 1.2 *Let C/K be a curve of genus $\geqslant 1$, and let $Q_0 \in C(K)$. Let J be the Jacobian of C and suppose $J(K) = \{0_J\}$. Let $\mathfrak{p}$ be a finite prime of $\mathcal{O}_K$ of good reduction for C. Let L/K be an extension of degree m. Suppose that*

(i) *$\mathfrak{p}$ is totally ramified in L;*
(ii) $\gcd(\# J(\mathbb{F}_{\mathfrak{p}}), m) = 1$.

Then $(C \setminus \{Q_0\})(\mathcal{O}_{L,S}) = \emptyset$ for any set of places S not containing $\mathfrak{P}$.

Proof If $Q \in (C \setminus \{Q_0\})(\mathcal{O}_{L,S})$ then the linear equivalence class $[Q - Q_0]$ yields an element of $(J \setminus \{0_J\})(\mathcal{O}_{L,S})$, contradicting Theorem 1.1. □

We refer to [7, Theorem 4] for an analogue of Corollary 1.2 in the context of integral points on $\mathbb{P}^1 \setminus \{0, 1, \infty\}$.

Example 1.3 Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by an order in an imaginary quadratic field K. Let p be a prime of good supersingular reduction for E, and write K_n for the n-th layer of the anticyclotomic $\mathbb{Z}_p$-extension of K. It is known [9, Theorem 1.8] that $E(K_n)$ has unbounded rank as $n \to \infty$. Indeed $\text{rank}\,(E_{K_n}) - \text{rank}\,(E_{K_{n-2}}) = 2p^{n-1}(p-1)$ for sufficiently large n.

Suppose now that p is unramified in K. As $E/\mathbb{F}_p$ is supersingular, we know that p is inert in K. Write $\mathfrak{p} = p\mathcal{O}_K$ for the unique prime of $\mathcal{O}_K$ above p. Since $E/\mathbb{F}_p$ is supersingular, $a_\mathfrak{p}(E) \equiv 0 \pmod{p}$, where $a_\mathfrak{p}(E)$ denotes the trace of Frobenius of E at $\mathfrak{p}$. Thus $\# E(\mathbb{F}_\mathfrak{p}) \equiv 1 \pmod{p}$. In particular, $p \nmid \# E(\mathbb{F}_\mathfrak{p})$.

Let $n \geqslant 1$. By [11, Theorem 1], the extension K_n/K is unramified away from $\mathfrak{p}$. We show that $\mathfrak{p}$ is totally ramified in K_n. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_{K_n}$ above $\mathfrak{p}$, and let $I_\mathfrak{P} \subseteq \text{Gal}\,(K_n/K)$ be the inertia group. As K_n/K is cyclic, $I_\mathfrak{P}$ is a normal subgroup. In particular, $I_\mathfrak{P} = I_{\mathfrak{P}'}$ for any other prime ideal $\mathfrak{P}'$ of $\mathcal{O}_{K_n}$ above $\mathfrak{p}$. It follows that the fixed field $K_n^{I_\mathfrak{P}}$ is an unramified cyclic extension of K. However, K is the CM field of an elliptic curve defined over $\mathbb{Q}$ and so [23, Theorem II.4.3] it has class number 1. Therefore $K_n^{I_\mathfrak{P}} = K$, implying $I_\mathfrak{P} = \text{Gal}\,(K_n/K)$, and so $\mathfrak{p}$ is totally ramified in K.

Finally we suppose that $E(K) = \{0_E\}$. It now follows from Theorem 1.1 that $(E \setminus \{0_E\})(\mathcal{O}_{K_n}) = \varnothing$ for all $n \geqslant 1$, despite the fact that the rank of $E(K_n)$ is unbounded as $n \to \infty$.

As a very concrete example of the above, let $E/\mathbb{Q}$ be the elliptic curve with Cremona label `432a1` and Weierstrass model

$$E: \; Y^2 = X^3 - 16.$$

This has conductor $432 = 2^4 \times 3^3$, and has CM by the ring of integers of $K = \mathbb{Q}(\sqrt{-3})$. We checked using the computer algebra system `Magma` [2] that $E(K) = \{0_E\}$. Let p be an odd prime $\equiv 2 \pmod 3$. Then p is a prime of good supersingular reduction for E, and for every $n \geqslant 1$, we have $(E \setminus \{0_E\})(\mathcal{O}_{K_n}) = \varnothing$ where K_n is the n-th layer of anticyclotomic $\mathbb{Z}_p$-extension of K.

Remark In view of the above, it is interesting to ask if a "positive proportion" of CM elliptic curves $E/\mathbb{Q}$ satisfy $E(K) = \{0_E\}$, where K is the field of complex multiplication. We rephrase this question a little more precisely. By the Baker–Heegner–Stark theorem on imaginary quadratic fields of class number 1, we know that there are 13 CM j-invariants belonging to $\mathbb{Q}$; for a list see [23, p. 483]. Let j be one of these 13 j-invariants and write $\mathcal{E}(j)$ for the family of elliptic curve $E/\mathbb{Q}$ (all twists of each other) with this j-invariant, ordered by conductor. Let K be the common CM field for $E \in \mathcal{E}(j)$. Is there a positive proportion of $E \in \mathcal{E}(j)$ satisfying $E(K) = \{0_E\}$?

Throughout the paper ζ_r denotes a primitive r-th root of 1.

Corollary 1.4 *Let $A/\mathbb{Q}$ be an abelian variety satisfying $A(\mathbb{Q}) = \{0_A\}$, and write $\mathcal{N}_A$ for the conductor of A. Let*

$$R_A = \left\{p \nmid \mathcal{N}_A \text{ is prime} : \gcd(p(p-1), \# A(\mathbb{F}_p)) = 1\right\}.$$

Then $(A \setminus \{0_A\})(\mathbb{Z}[\zeta_{p^n}]) = \varnothing$ for all $p \in R_A$ and $n \geqslant 1$.

Proof Let $p \in R_A$ and write $L = \mathbb{Q}[\zeta_{p^n}]$. Then p is totally ramified in L, and as $p \nmid \mathcal{N}_A$, it is a prime of good reduction for A. Moreover, $[L:\mathbb{Q}] = p^{n-1}(p-1)$ is coprime to $\# A(\mathbb{F}_p)$. The conclusion follows from Theorem 1.1. □

The set R_A can be finite or empty. For example if A has a rational point of order 2 then $2 \mid \# A(\mathbb{F}_p)$ for all odd primes of good reduction, and so $R_A \subseteq \{2\}$ in this case. In a forthcoming paper we provide heuristic and experimental evidence that R_A has positive density under some conditions on A. For now we content ourselves with two examples.

Example 1.5 Let $E/\mathbb{Q}$ be the elliptic curve with `LMFDB` [25] label `67.a1` and Cremona label `67a1`. This has Weierstrass model

$$E: \; Y^2 + Y = X^3 + X^2 - 12X - 21, \tag{1}$$

conductor 67 and Mordell–Weil group $E(\mathbb{Q}) = \{0_E\}$. By Corollary 1.4, the affine Weierstrass model (1) does not have any $\mathbb{Z}[\zeta_{p^n}]$-points for the values of $p \in R_E$. For a positive integer N we shall write $[1, N]$ for the interval consisting of integers up to N. A short `Magma` computation shows that

$$\begin{aligned} R_E \cap [1, 1000] = \{&2, 17, 19, 23, 47, 59, 89, 107, 127, 149, 151, 157, 163, \\ &173, 193, 199, 227, 257, 283, 359, 421, 431, 449, 479, \\ &491, 509, 569, 601, 613, 617, 659, 691, 719, 773, 821, \\ &823, 827, 839, 881, 887, 911, 947, 953, 971, 977\}. \end{aligned}$$

Table 1 gives some statistics.

Example 1.6 Let $C/\mathbb{Q}$ be the genus 2 curve with `LMFDB` label `8969.a.8969.1` having affine Weierstrass model

$$C: \; y^2 + (x+1)y = x^5 - 55x^4 - 87x^3 - 54x^2 - 16x - 2. \tag{2}$$

We take $A = J$ to be the Jacobian of C. According to the `LMFDB`, J is absolutely simple, and $J(\mathbb{Q}) = \{0_J\}$. The conductor is $\mathcal{N}_J = 8969$ which is prime. We note that C has a rational point at ∞, and thus $C(\mathbb{Q}) = \{\infty\}$. By Corollary 1.4, $(J \setminus \{0_J\})(\mathbb{Z}[\zeta_{p^n}]) = \varnothing$ for all $p \in R_J$, and so the affine Weierstrass model in (2) has no $\mathbb{Z}[\zeta_{p^n}]$-points for all $n \geqslant 1$. A short `Magma` computation gives

$$\begin{aligned} R_J \cap [1, 1000] = \{&11, 13, 43, 79, 149, 163, 223, 227, 269, 353, 367, 443, \\ &523, 593, 641, 683, 743, 769, 797, 887, 929, 941, 991\}. \end{aligned}$$

Table 1 We write $\pi(N)$ for the number of primes $\leqslant N$. This table gives statistics for $R_E \cap [1, 10^k]$ for $2 \leqslant k \leqslant 8$, where E is the elliptic curve `67a1`

k	$\# R_E \cap [1, 10^k]$	$\pi(10^k)$	$(\# R_E \cap [1, 10^k])/\pi(10^k)$ (4 d.p.)
2	7	25	0.2800
3	45	168	0.2679
4	297	1229	0.2417
5	2309	9592	0.2407
6	19060	78498	0.2428
7	160958	664579	0.2422
8	1395958	5761455	0.2423

Note $\# R_J \cap [1, 1000] = 23$, $\pi(1000) = 168$, and so $(\# R_J \cap [1, 1000])/\pi(1000) \approx 0.137$.

Our next theorem concerns abelian varieties A defined over $\mathbb{Q}$ with trivial Mordell–Weil group; i.e. $A(\mathbb{Q}) = \{0_A\}$. Let ℓ be a rational prime, and let S be a finite set of rational primes (we allow $\ell \in S$ and also $\ell \notin S$). The theorem states that, under an additional hypothesis, $(A \setminus \{0_A\})(\mathcal{O}_{L,S}) = \varnothing$ for 100% of degree ℓ cyclic extensions $L/\mathbb{Q}$, ordered by conductor. Here $\mathcal{O}_{L,S}$ denotes $\mathcal{O}_{L,T}$ where T is set of places of L above the rational primes belonging to S. We denote by ζ_ℓ a fixed primitive ℓ-th root of 1, and by $A[\ell]$ the ℓ-torsion subgroup of $A(\overline{\mathbb{Q}})$. We observe that $\mathbb{Q}(\zeta_\ell) \subseteq \mathbb{Q}(A[\ell])$ (for a proof see Lemma 5.1 below). We shall write

$$G_\ell(A) = \mathrm{Gal}\,(\mathbb{Q}(A[\ell])/\mathbb{Q}), \quad H_\ell(A) = \mathrm{Gal}\,(\mathbb{Q}(A[\ell])/\mathbb{Q}(\zeta_\ell)). \tag{3}$$

We note that $H_\ell(A)$ is a normal subgroup of $G_\ell(A)$. We also write

$$\mathcal{C}_\ell(A) = \big\{\sigma \in H_\ell(A) : \sigma \text{ acts freely on } A[\ell]\big\}. \tag{4}$$

Theorem 1.7 *Let ℓ be a rational prime. Let A be an abelian variety defined over $\mathbb{Q}$. Suppose that*

(i) $A(\mathbb{Q}) = \{0_A\}$*;*
(ii) $\mathcal{C}_\ell(A) \neq \varnothing$.

For $X > 0$, let $\mathcal{F}_\ell^{\mathrm{cyc}}(X)$ be set of cyclic number fields L of degree ℓ and conductor at most X. Let S be a finite set of rational primes. Then

$$\frac{\#\{L \in \mathcal{F}_\ell^{\mathrm{cyc}}(X) : (A \setminus \{0_A\})(\mathcal{O}_{L,S}) \neq \varnothing\}}{\# \mathcal{F}_\ell^{\mathrm{cyc}}(X)} = O\left(\frac{1}{(\log X)^\gamma}\right)$$

as $X \to \infty$, where

$$\gamma = \frac{\# \mathcal{C}_\ell(A)}{\# H_\ell(A)}.$$

Remark • Theorem 1.7 was inspired by [8] which studies the solutions to the unit equation over families of cyclic number fields of prime degree.

- Let $L/\mathbb{Q}$ be cyclic of prime degree ℓ. Write N for the conductor of L, and Δ for its absolute discriminant. It easily follows from the discriminant-conductor formula [28, Theorem 3.11] that $\Delta = N^{\ell-1}$. The conclusion of Theorem 1.7 is therefore unchanged if instead we let $\mathcal{F}_\ell^{\mathrm{cyc}}(X)$ be the set of cyclic degree ℓ number fields with absolute discriminant at most X.

Condition (ii) of Theorem 1.7, in its present form, is computationally unfriendly. The following lemma simplifies the task of checking condition (ii).

Lemma 1.8 *Let $p \neq \ell$ be a rational prime of good reduction for A. Write $\sigma_p \in G_\ell(A)$ for a Frobenius element at p.*

(a) $\sigma_p \in H_\ell(A)$ *if and only if* $p \equiv 1 \pmod{\ell}$.
(b) $\sigma_p \in \mathcal{C}_\ell(A)$ *if and only if* $p \equiv 1 \pmod{\ell}$ *and* $\ell \nmid \# A(\mathbb{F}_p)$.

Proof Let $p \neq \ell$ be a prime of good reduction for A. Recall that the isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q}) \cong (\mathbb{Z}/\ell\mathbb{Z})^\times$ sends the Frobenius element at a prime $q \neq \ell$ to the congruence class of q modulo ℓ. However, $\mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q}) \cong G_\ell(A)/H_\ell(A)$, thus $\sigma_p \in H_\ell(A)$ if and only if $p \equiv 1 \pmod{\ell}$. Write P_p for the characteristic polynomial of Frobenius at p acting on the ℓ-adic Tate module $T_\ell(A)$, and denote its reduction modulo ℓ by $\overline{P_p}(X) \in \mathbb{F}_\ell[X]$. We know [16, Theorem 19.1] that $\# A(\mathbb{F}_p) = P_p(1)$. Thus $\ell \mid \# A(\mathbb{F}_p)$ if and only if 1 is a root of $\overline{P_p}(X)$. This is equivalent to $1 \in \mathbb{F}_\ell$ being an eigenvalue for the action of σ_p on the $\mathbb{F}_\ell$-vector space $A[\ell]$, which is equivalent to σ_p failing to act freely on $A[\ell]$. □

Lemma 1.8 gives a computational method for verifying condition (ii) of Theorem 1.7 for a given prime ℓ: all we need to do is produce a prime $p \equiv 1 \pmod{\ell}$ such that $\ell \nmid \# A(\mathbb{F}_p)$. To check that condition (ii) holds for all primes ℓ, or all but finitely many primes ℓ, the following lemma can be useful.

Lemma 1.9 *Let $A/\mathbb{Q}$ be a principally polarized abelian variety of dimension d. Let ℓ be a rational prime and write*

$$\overline{\rho}_{A,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GSp}_{2d}(\mathbb{F}_\ell)$$

for the mod ℓ *representation of A. Suppose $\overline{\rho}_{A,\ell}$ is surjective. Then $\mathcal{C}_\ell(A) \neq \emptyset$.*

Proof Suppose $\overline{\rho}_{A,\ell}$ is surjective. The map $\overline{\rho}_{A,\ell}$ factors through $G_\ell(A)$. The image of $H_\ell(A) \subseteq G_\ell(A)$ is $\mathrm{Sp}_{2d}(\mathbb{F}_\ell)$. An element $\sigma \in H_\ell(A)$ acts freely on $A[\ell]$ if and only if its image in $\mathrm{Sp}_{2d}(\mathbb{F}_\ell)$ is a matrix with none of the eigenvalues equal to $1 \in \mathbb{F}_\ell$. All that remains is to specify such a matrix $M \in \mathrm{Sp}_{2d}(\mathbb{F}_\ell)$. If $\ell \neq 2$ we may take

$M = -I_{2d}$ where I_{2d} is the $2d \times 2d$ identity matrix. If $\ell = 2$ then we may take

$$M = \begin{pmatrix} 1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

□

It follows, thanks to the following theorem of Serre [20, Theorem 3], that condition (ii) of Theorem 1.7 is satisfied for all sufficiently large ℓ subject to some further assumptions on A.

Theorem 1.10 (Serre) *Let A be a principally polarized abelian variety of dimension d, defined over $\mathbb{Q}$. Assume that $d = 2, 6$ or d is odd and furthermore assume that* $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$*. Then there exists a bound B_A such that for all primes $\ell > B_A$ the representation $\overline{\rho}_{A,\ell}$ is surjective.*

Example 1.11 We return to the elliptic curve E in Example 1.5. We noted previously that $E(\mathbb{Q}) = \{0_E\}$. According to the LMFDB, $\overline{\rho}_{E,\ell}$ is surjective for all primes ℓ. It follows from Lemma 1.9 and Theorem 1.7 that for any prime ℓ, and any fixed set of rational primes S, the Weierstrass model (1) does not have $\mathcal{O}_{L,S}$-integral points, for 100% of cyclic degree ℓ number fields L.

Example 1.12 We return to the genus 2 curve C in Example 1.6 and to its Jacobian J. We observed previously that $J(\mathbb{Q}) = \{0_J\}$. In particular, J satisfies hypothesis (i) of Theorem 1.7. Moreover, J is semistable as its conductor $\mathcal{N}_J = 8969$ is prime. Using the method in [1, 5] (which is particularly suited to semistable Jacobians), we checked that $\overline{\rho}_{J,\ell}$ is surjective for $\ell \geqslant 5$, $\ell \neq 8969$. Thus, by Lemma 1.9, the Jacobian J satisfies hypothesis (ii) of Theorem 1.7 for those primes. For $\ell = 2, 3, 8969$ we choose $p = 5, 7, 17939$ respectively (all three satisfying $p \equiv 1 \pmod{\ell}$), and find

$$\# J(\mathbb{F}_5) = 15, \quad \# J(\mathbb{F}_7) = 32, \quad \# J(\mathbb{F}_{17939}) = 317816600 = 2^3 \times 5^2 \times 1589083,$$

so, by Lemma 1.8, hypothesis (ii) of the theorem is satisfied for $\ell = 2, 3$ and 8969. It follows from Theorem 1.7 that for all primes ℓ, and any finite set of primes S, we have $(J \setminus \{0_J\})(\mathcal{O}_{L,S}) = \varnothing$ for 100% of cyclic degree ℓ number fields L. We conclude that $(C \setminus \{\infty\})(\mathcal{O}_{L,S}) = \varnothing$ for 100% of cyclic degree ℓ number fields L.

The paper is organized as follows. In Sect. 2, we study traces on abelian varieties over totally ramified local extensions. In Sect. 3 we prove Theorem 1.1. Sect. 4 is devoted to counting cyclic fields of prime degree ℓ such that the conductor is divisible only by primes belonging a certain 'regular' set. Section 5 gives a proof of Theorem 1.7.

2 Traces over totally ramified local extensions

In this section, we let p be a rational prime, and K a finite extension of $\mathbb{Q}_p$, and L/K a totally ramified extension of finite degree m. Let π and Π be uniformizing elements for K and L respectively. Let M/K be the Galois closure of L/K. Let $|\cdot|$ denote the absolute value on these fields normalised so that $|p| = p^{-1}$. Write $\sigma_1, \dots, \sigma_m$ for the distinct embeddings $L \hookrightarrow M$ satisfying $\sigma_i(a) = a$ for $a \in K$, where σ_1 is the trivial embedding $\sigma_1(\alpha) = \alpha$ for $\alpha \in L$.

Lemma 2.1 *Let $\alpha \in \mathcal{O}_L$. Then $|\sigma_i(\alpha) - \alpha| < 1$ for $i = 1, \dots, m$.*

Proof As L/K is totally ramified we have $\mathcal{O}_L/\Pi = \mathcal{O}_K/\pi$. Hence there is some $a \in \mathcal{O}_K$ such that $\alpha \equiv a \pmod{\Pi}$. It follows that $|\alpha - a| < 1$. Now, as each σ_i is the restriction to L of an automorphism of M/K, the differences $\alpha - a$ and $\sigma_i(\alpha) - a$ are conjugate over K. Therefore, by [4, p. 119], $|\sigma_i(\alpha) - a| = |\alpha - a| < 1$. By the ultrametric property of non-archimedean absolute values, $|\sigma_i(\alpha) - \alpha| < 1$. ◻

Lemma 2.2 *Let A/K be an abelian variety having good reduction. Let $Q \in A(L)$. Then*

$$\mathrm{Trace}_{L/K}\, Q \equiv mQ \pmod{\Pi}. \tag{5}$$

Proof We first prove (5) under the additional assumption that $L = K(Q)$. Let $Q_i = \sigma_i(Q) \in A(M)$ with $Q = Q_1$. The assumption $L = K(Q)$ ensures $Q_1, \dots, Q_m$ are distinct as well as being a single Galois orbit over K, and so allows us to interpret the m-tuple $\{Q_1, \dots, Q_m\}$ as a closed K-point on A. As A has good reduction, it extends to an abelian scheme $\mathcal{A}$ over $\mathrm{Spec}\,(\mathcal{O}_K)$, and the closed K-point $\{Q_1, \dots, Q_m\}$ extends to a $\mathrm{Spec}\,(\mathcal{O}_K)$-point on $\mathcal{A}$ that we denote by $\mathcal{Q}$. We take an affine patch $\mathrm{Spec}\,(\mathcal{O}_K[x_1, \dots, x_n]/(f_1, \dots, f_r))$ of $\mathcal{A}$ containing $\mathcal{Q}$. In this patch we can identify Q with a point $Q = (q_1, \dots, q_n) \in \mathcal{O}_L^n$ satisfying $f_1(q_1, \dots, q_n) = \cdots = f_r(q_1, \dots, q_n) = 0$. Then $Q_i = (\sigma_i(q_1), \dots, \sigma_i(q_n))$. Let ϖ be a uniformizing element for M. Then $\sigma_i(q_j) \equiv q_j \pmod{\varpi}$ by Lemma 2.1. Thus $Q_i \equiv Q \pmod{\varpi}$. Hence

$$\mathrm{Trace}_{L/K}\, Q = \sum_{i=1}^{m} Q_i \equiv mQ \pmod{\varpi}.$$

Now (5) follows as both $\mathrm{Trace}_{L/K}\, Q$ and mQ belong to $A(L)$.

For the general case, let $L' = K(Q) \subseteq L$, $m' = [L' : K]$ and Π' be a uniformizer for L'. Then, by the above,

$$\mathrm{Trace}_{L'/K}\, Q \equiv m'Q \pmod{\Pi'}.$$

Therefore

$$\mathrm{Trace}_{L/K}\, Q = \mathrm{Trace}_{L/L'}(\mathrm{Trace}_{L'/K}\, Q) \equiv [L : L'] \cdot m'Q = mQ \pmod{\Pi'}.$$

The lemma follows as $\Pi \mid (\Pi' \cdot \mathcal{O}_L)$. ◻

3 Proof of Theorem 1.1

With notation and assumptions as in the statement of Theorem 1.1, let $Q \in A(L)$. Then $\mathrm{Trace}_{L/K}(Q) \in A(K)$. However, by assumption, $A(K) = \{0_A\}$, and so $\mathrm{Trace}_{L/K}(Q) = 0_A$. By Lemma 2.2 we have

$$mQ \equiv \mathrm{Trace}_{L/K}(Q) \pmod{\mathfrak{P}}.$$

Thus $mQ \equiv 0_A \pmod{\mathfrak{P}}$. But, since $\mathfrak{p}$ is totally ramified, $\mathbb{F}_{\mathfrak{P}} = \mathbb{F}_{\mathfrak{p}}$, and so $A(\mathbb{F}_{\mathfrak{P}}) = A(\mathbb{F}_{\mathfrak{p}})$. It follows from assumption (ii) of the statement of the theorem that $Q \equiv 0_A \pmod{\mathfrak{P}}$. Thus $Q \in A^1(L_{\mathfrak{P}})$ completing the proof.

4 Counting cyclic fields

Let $\mathbb{P}$ be the set of prime numbers and let $\mathcal{P} \subseteq \mathbb{P}$. Following Serre [18], we call $\mathcal{P}$ *regular of density* $\alpha > 0$ if

$$\sum_{p \in \mathcal{P}} \frac{1}{p^s} = \alpha \cdot \log\left(\frac{1}{s-1}\right) + \theta_A(s) \tag{6}$$

where θ_A extends to a holomorphic function on $\mathrm{Re}(s) \geqslant 1$. We call the set $\mathcal{P}$ *Frobenian of density* $\alpha > 0$ if there exists a finite Galois extension $L/\mathbb{Q}$ and a subset $\mathcal{C}$ of $G = \mathrm{Gal}\,(L/\mathbb{Q})$, such that

- $\mathcal{C}$ is a union of conjugacy classes in G;
- $\alpha = \#\,\mathcal{C}/\#\,G$;
- for every sufficiently large prime p, we have $p \in \mathcal{P}$ if and only if $\sigma_p \in \mathcal{C}$ where σ_p is a Frobenius element of G corresponding to p.

By the Chebotarev Density Theorem [18, Proposition 1.5], if $\mathcal{P}$ is Frobenian of density $\alpha > 0$ then it is regular of density $\alpha > 0$.

Let ℓ be a rational prime, and let

$$\mathbb{P}_\ell = \{\ell\} \cup \{p : p \text{ is prime } \equiv 1 \pmod{\ell}\}. \tag{7}$$

The purpose of this section is to prove the following proposition which will be needed for the proof of Theorem 1.7.

Proposition 4.1 *Let $\mathcal{P} \subseteq \mathbb{P}_\ell$ and suppose $\mathcal{P}$ is regular of density $\alpha > 0$. For $X > 0$ let $\mathcal{F}^{\mathrm{cyc}}_{\mathcal{P},\ell}(X)$ be the set of number fields L such that:*

(i) *L is cyclic of degree ℓ;*
(ii) *the conductor of L is divisible only by primes belonging to $\mathcal{P}$;*
(iii) *the conductor of L is at most X.*

There is some $c > 0$ such that

$$\#\,\mathcal{F}^{\mathrm{cyc}}_{\mathcal{P},\ell}(X) \sim c \cdot \frac{X}{(\log X)^{1-\beta}},$$

as $X \to \infty$*, where* $\beta = \alpha \cdot (\ell - 1)$.

Remark (I) The method of proof does not yield a convenient formula for the constant c in the above asymptotic estimate. See the remark at the end of the section.

(II) By Lemma 4.6 below, $\mathcal{F}^{\mathrm{cyc}}_{\mathbb{P}_\ell,\ell}(X) = \mathcal{F}^{\mathrm{cyc}}_{\ell}(X)$ is the set of all degree ℓ cyclic number fields of conductor at most X. By Dirichlet's Theorem, the set $\mathbb{P}_\ell$ is regular of density $1/(\ell-1)$. The proposition is saying in this case that

$$\# \mathcal{F}^{\mathrm{cyc}}_{\ell}(X) \sim cX$$

as $X \to \infty$. This is in fact a theorem of Urazbaev [26]. A proof can also be found in [17, Sect. 2.2], and a generalization to more general abelian extensions in [29]. Lemmas 4.2, 4.3, 4.4, 4.5, 4.6 below are in essence well-known, and can be found in some form or other scattered across the literature, e.g. [14, Section 1], [17, Section 2.2]. It however seemed more convenient to prove them from scratch.

Let G be a finite abelian group, for now written additively. Let ℓ be a prime. We define the *ℓ-rank of* G to be the dimension of the $\mathbb{F}_\ell$-vector space $G/\ell G$.

Lemma 4.2 *Let r be the ℓ-rank of G. Then the number of subgroups of index ℓ in G is* $(\ell^r - 1)/(\ell - 1)$.

Proof Any subgroup H of G of index ℓ contains ℓG. Thus there is a 1-1 correspondence between subgroups of index ℓ in G and subgroups of index ℓ in $G/\ell G$, or equivalently $\mathbb{F}_\ell$-subspaces of $G/\ell G$ of codimension 1. But, regarded as an $\mathbb{F}_\ell$-vector space, $G/\ell G$ is isomorphic to $\mathbb{F}_\ell^r$. The codimension 1 subspaces of $\mathbb{F}_\ell^r$ correspond to points in $\check{\mathbb{P}}^{r-1}(\mathbb{F}_\ell)$, where $\check{\mathbb{P}}^{r-1}$ denotes the projective space dual to $\mathbb{P}^{r-1}$. However, $\check{\mathbb{P}}^{r-1} \cong \mathbb{P}^{r-1}$. The lemma follows. □

Let $M(n)$ denote the number of degree ℓ cyclic fields contained in $\mathbb{Q}(\zeta_n)$. Let $N(n)$ denote the number of degree ℓ cyclic fields of conductor n. Then

$$M(n) = \sum_{d \mid n} N(d). \tag{8}$$

Lemma 4.3 *Let n be a positive integer. Write $r_\ell(n)$ for the ℓ-rank of $(\mathbb{Z}/n\mathbb{Z})^\times$. Then*

$$M(n) = \frac{\ell^{r_\ell(n)} - 1}{\ell - 1}.$$

Proof By the Galois correspondence, $M(n)$ is the number of index ℓ subgroups in

$$\mathrm{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

The lemma follows from Lemma 4.2. □

Lemma 4.4 *Let q be a prime and $\alpha \geqslant 1$. Then*

$$r_\ell(q^\alpha) = \begin{cases} 1 & \textit{if } q \equiv 1 \pmod{\ell}, \\ 1 & \textit{if } q = \ell \neq 2 \textit{ and } \alpha \geqslant 2, \\ 1 & \textit{if } q = \ell = 2 \textit{ and } \alpha = 2, \\ 2 & \textit{if } q = \ell = 2 \textit{ and } \alpha \geqslant 3, \\ 0 & \textit{in all other cases.} \end{cases}$$

Proof If $q \neq 2$ then $(\mathbb{Z}/q^\alpha\mathbb{Z})^\times$ is cyclic of order $(q-1)q^{\alpha-1}$. Thus $r_\ell(q^\alpha) = 0$ unless $q \equiv 1 \pmod{\ell}$ or $q = \ell$ and $\alpha \geqslant 2$, in which case $r_\ell(q^\alpha) = 1$.

Suppose $q = 2$. Then

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \cong \begin{cases} 0, & \alpha = 1, \\ \mathbb{Z}/2\mathbb{Z}, & \alpha = 2, \\ (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha-2}\mathbb{Z}), & \alpha \geqslant 3. \end{cases}$$

The lemma follows. □

Lemma 4.5 *If m_1, m_2 are positive integers and* $\gcd(m_1, m_2) = 1$ *then*

$$r_\ell(m_1 m_2) = r_\ell(m_1) + r_\ell(m_2).$$

Proof By the Chinese Remainder Theorem, $(\mathbb{Z}/m_1m_2\mathbb{Z})^\times \cong (\mathbb{Z}/m_1\mathbb{Z})^\times \times (\mathbb{Z}/m_2\mathbb{Z})^\times$. The lemma follows. □

Lemma 4.6 *Let n be the conductor of a cyclic field of degree ℓ. Then*

$$n = \ell^v \cdot \prod_{i=1}^{t} q_i \tag{9}$$

where $q_1, \ldots, q_t$ are distinct primes $\equiv 1 \pmod{\ell}$ *and*

$$v = \begin{cases} 0 \textit{ or } 2 & \textit{if } \ell \neq 2, \\ 0, 2 \textit{ or } 3 & \textit{if } \ell = 2. \end{cases}$$

Moreover,

$$N(n) = \begin{cases} (\ell-1)^{t-1} & \textit{if } v = 0, \\ (\ell-1)^t & \textit{if } v = 2, \\ \ell(\ell-1)^t & \textit{if } \ell = 2 \textit{ and } v = 3. \end{cases}$$

Proof Applying Möbius inversion to (8) we have

$$N(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \cdot M(d).$$

From Lemma 4.3, and using the fact that $\sum_{d|n} \mu(n/d) = 0$ for $n > 1$ we have

$$N(n) = \frac{1}{\ell - 1} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \cdot \ell^{r_\ell(d)}. \tag{10}$$

Now the function $g(m) := \ell^{r_\ell(m)}$ is multiplicative by Lemma 4.5. Therefore the convolution $\mu * g$ is also multiplicative. Note that (10) may be re-expressed as $(\ell - 1)N(n) = (\mu * g)(n)$. Thus

$$(\ell - 1)N(n) = \prod_{q^\alpha \,||\, n} (\mu * g)(q^\alpha),$$

where the product is taken over prime powers q^α dividing n exactly. In particular, since n is the conductor of a cyclic degree ℓ field, $N(n) \neq 0$, and so $(\mu * g)(q^\alpha) \neq 0$ for all $q^\alpha \;||\; n$.

Now let $q \neq \ell$ and $\alpha \geqslant 1$. Then

$$(\mu * g)(q^\alpha) = \ell^{r_\ell(q^\alpha)} - \ell^{r_\ell(q^{\alpha-1})} = \begin{cases} \ell - 1 & \text{if} \;\; q \equiv 1 \pmod{\ell} \;\; \text{and} \;\; \alpha = 1, \\ 0 & \text{if} \;\; q \not\equiv 1 \pmod{\ell} \;\; \text{or} \;\; \alpha \geqslant 2 \end{cases}$$

by Lemma 4.4. It follows that n satisfies (9) where the q_i are distinct primes $\equiv 1 \pmod{\ell}$ and that

$$N(n) = (\ell - 1)^{t-1} \cdot (\mu * g)(\ell^v).$$

Finally

$$(\mu * g)(\ell^v) = \begin{cases} 1 & \text{if} \;\; v = 0, \\ \ell - 1 & \text{if} \;\; v = 2, \\ \ell^2 - \ell & \text{if} \;\; \ell = 2 \;\; \text{and} \;\; v = 3, \\ 0 & \text{in all other cases,} \end{cases}$$

again from Lemma 4.4. This completes the proof. ◻

Lemma 4.7 *Let ℓ be a prime. Let $\mathcal{P} \subseteq \mathbb{P}$ be regular of density $\alpha > 0$. Suppose that all primes in $\mathcal{P}$ are $\equiv 1 \pmod{\ell}$. Let $\mathcal{B}$ be the set of all squarefree positive integers with prime divisors belonging entirely to $\mathcal{P}$. Denote by $\omega(n)$ the number of distinct prime* *divisors of an integer n. Then there is some* $\kappa > 0$ *such that*

$$\sum_{\substack{n \in \mathcal{B} \\ n \leqslant X}} (\ell - 1)^{\omega(n)} \sim \kappa \cdot \frac{X}{(\log X)^{1-\beta}}$$

as $X \to \infty$*, where* $\beta = \alpha \cdot (\ell - 1)$.

Proof Consider the Dirichlet series

$$D(s) := \sum_{n \in \mathcal{B}} \frac{(\ell - 1)^{\omega(n)}}{n^s} = \prod_{p \in \mathcal{P}} \left(1 + \frac{\ell - 1}{p^s}\right).$$

Then

$$\log D(s) = \sum_{p \in \mathcal{P}} \frac{\ell - 1}{p^s} + \theta(s)$$

where θ is holomorphic on $\mathrm{Re}(s) > 1/2$. By (6),

$$\log D(s) = \beta \cdot \log\left(\frac{1}{s-1}\right) + \phi(s) \tag{11}$$

and ϕ is holomorphic on $\mathrm{Re}(s) \geqslant 1$. Thus

$$D(s) = \frac{\Phi(s)}{(s-1)^{\beta}}$$

where $\Phi(s) = \exp(\phi(s))$ is holomorphic and non-zero on $\mathrm{Re}(s) \geqslant 1$. Since $\mathcal{P}$ is contained in the set of primes $\equiv 1 \pmod{\ell}$ we know that $0 < \alpha \leqslant 1/(\ell - 1)$, and so $0 < \beta \leqslant 1$.

We now apply to $D(s)$ a variant of Ikehara's Tauberian theorem due to Delange [24, Theorem II.7.28] to obtain

$$\sum_{\substack{n \in \mathcal{B} \\ n \leqslant X}} (\ell - 1)^{\omega(n)} \sim \frac{\Phi(1)}{\Gamma(\beta)} \cdot \frac{X}{(\log X)^{1-\beta}},$$

where Γ denotes the gamma function. The lemma follows, where

$$\kappa = \frac{\Phi(1)}{\Gamma(\beta)} = \frac{\exp(\phi(1))}{\Gamma(\beta)}. \tag{12}$$

□

Proof of Proposition 4.1 Suppose first that $\ell \notin \mathcal{P}$, and let $\mathcal{B}$ be as in the statement of Lemma 4.7. Then, by Lemma 4.6,

$$\# \mathcal{F}_{\mathcal{P},\ell}^{\text{cyc}}(X) = \sum_{\substack{n \in \mathcal{B} \\ n \leqslant X}} N(n) = \frac{1}{\ell - 1} \sum_{\substack{n \in \mathcal{B} \\ n \leqslant X}} (\ell - 1)^{\omega(n)}. \tag{13}$$

The proposition follows immediately from Lemma 4.7 in this case. Suppose next that $\ell \in \mathcal{P}$ and $\ell \neq 2$. Let $\mathcal{P}' = \mathcal{P} \setminus \{\ell\}$ and now let $\mathcal{B}$ be the set of all squarefree positive integers with prime divisors belonging entirely to $\mathcal{P}'$. By Lemma 4.6

$$\# \mathcal{F}_{\mathcal{P},\ell}^{\text{cyc}}(X) = \sum_{\substack{n \in \mathcal{B} \\ n \leqslant X}} N(n) + \sum_{\substack{n \in \mathcal{B} \\ n \leqslant X/\ell^2}} N(\ell^2 n) = \sum_{\substack{n \in \mathcal{B} \\ n \leqslant X}} (\ell - 1)^{\omega(n)-1} + \sum_{\substack{n \in \mathcal{B} \\ n \leqslant X/\ell^2}} (\ell - 1)^{\omega(n)}.$$

The proposition follows from Lemma 4.7 in this case also. The case $\ell = 2 \in \mathcal{P}$ is dealt with similarly. □

Remark The constant c in the statement of Proposition 4.1 depends on the constant κ in the statement of Lemma 4.7. Let us consider the simplest case where $\ell \notin \mathcal{P}$. Then from (13) and (12) we have

$$c = \frac{\kappa}{\ell - 1} = \frac{\exp(\phi(1))}{(\ell - 1) \cdot \Gamma(\beta)}.$$

We do not see an explicit expression for $\phi(1)$. The best we can do, from (11), is to say

$$\phi(1) = \lim_{s \to 1^+} \left(\log D(s) - \beta \log\left(\frac{1}{s - 1} \right) \right).$$

5 Proof of Theorem 1.7

Let ℓ be a rational prime, and let $A/\mathbb{Q}$ be an abelian variety. The following result is stated as an exercise in [19, Section 4.6].

Lemma 5.1 $\mathbb{Q}(\zeta_\ell) \subseteq \mathbb{Q}(A[\ell])$.

Proof If A is principally polarized then the lemma is a famous consequence of the properties of the Weil pairing on $A[\ell]$. We learned the following more general argument from a `Mathoverflow` post by Yuri Zarhin [30]. Write $A^\vee$ for the dual abelian variety, and let $\phi \colon A \to A^\vee$ be a $\mathbb{Q}$-polarization of smallest possible degree. If $A[\ell] \subseteq \ker(\phi)$, then $P \mapsto \phi((1/\ell)P)$ is a well-defined $\mathbb{Q}$-polarization contradicting the minimality of the degree. Thus there is some $Q \in A[\ell]$ such that $\phi(Q) \in A^\vee[\ell] \setminus \{0_{A^\vee}\}$. The non-degeneracy of the Weil pairing $e_\ell \colon A[\ell] \times A^\vee[\ell] \to \langle \zeta_\ell \rangle$ ensures the existence of $P \in A[\ell]$ such that $e_\ell(P, \phi(Q)) = \zeta_\ell$. Now P and $\phi(Q)$ are fixed by $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(A[\ell]))$, and so, by the Galois-compatibility of the Weil pairing, ζ_ℓ is also fixed by $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(A[\ell]))$. Thus $\zeta_\ell \in \mathbb{Q}(A[\ell])$. □

We let $G_\ell(A)$, $H_\ell(A)$ be as in (3), and $\mathcal{C}_\ell(A)$ as in (4). We note that $\mathcal{C}_\ell(A)$ is a finite union of conjugacy classes. We now suppose that A and ℓ satisfy the hypotheses of Theorem 1.7, namely

(i) $A(\mathbb{Q}) = \{0_A\}$;
(ii) $\mathcal{C}_\ell(A) \neq \varnothing$.

Let S be a finite set of rational primes. Enlarge S so that it includes ℓ and all the primes of bad reduction for A. Let $\mathbb{P}_\ell$ be as in (7). Let

$$\mathcal{P} = \left\{p \in \mathbb{P}_\ell : p \in S \text{ or } \sigma_p \notin \mathcal{C}_\ell(A)\right\};$$

here, as in Lemma 1.8, $\sigma_p \in G_\ell(A)$ denotes a Frobenius element associated to p.

Lemma 5.2 *The set $\mathcal{P}$ is Frobenian (and therefore regular) of density*

$$\alpha := \frac{\# H_\ell(A) - \# \mathcal{C}_\ell(A)}{(\ell - 1) \cdot \# H_\ell(A)}. \tag{14}$$

Proof Let p be a sufficiently large prime. By part (a) of Lemma 1.8, we have $p \in \mathcal{P}$ if and only if $\sigma_p \in H_\ell(A) \setminus \mathcal{C}_\ell(A)$. Thus $\mathcal{P}$ is Frobenian of density

$$\frac{\# H_\ell(A) - \# \mathcal{C}_\ell(A)}{\# G_\ell(A)}.$$

The lemma follows as $G_\ell(A)/H_\ell(A) \cong \mathrm{Gal}\,(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})$ has order $\ell - 1$. □

Lemma 5.3 *Let $L/\mathbb{Q}$ be cyclic of degree ℓ and suppose $(A \setminus \{0_A\})(\mathcal{O}_{L,S}) \neq \varnothing$. Then the conductor of L is divisible only by primes belonging to $\mathcal{P}$.*

Proof We know from Lemma 4.6 that the prime divisors of the conductor of L belong to $\mathbb{P}_\ell$. Let $p \equiv 1 \pmod{\ell}$ be a prime of good reduction for A dividing the conductor of L. It is sufficient to show that $\sigma_p \notin \mathcal{C}_\ell(A)$. Suppose $\sigma_p \in \mathcal{C}_\ell(A)$. Since p divides the conductor of L it is ramified in L. However, $\mathrm{Gal}\,(L/\mathbb{Q})$ is cyclic of order ℓ. As the inertia subgroup at p is non-trivial it must equal $\mathrm{Gal}\,(L/\mathbb{Q})$. We deduce that p is totally ramified in L. Also, by Lemma 1.8, we have $\ell \nmid \# A(\mathbb{F}_p)$. Recall that $A(\mathbb{Q}) = \{0_A\}$ by assumption (i) above. We now apply Theorem 1.1 to conclude that $(A \setminus \{0_A\})(\mathcal{O}_{L,S}) = \varnothing$, giving a contradiction. □

Proof of Theorem 1.7

By assumption (ii) above $\mathcal{C}_\ell(A) \neq \varnothing$. It follows from (14) that $\alpha < 1/(\ell - 1)$. Moreover, from the definition of $\mathcal{C}_\ell(A)$ in (4), we note that $1 \in H_\ell(A)$ but $1 \notin \mathcal{C}_\ell(A)$. It follows that $\alpha > 0$. Lemma 5.2 tells us that $\mathcal{P}$ is regular of density α. By Lemma 5.3,

$$\left\{L \in \mathcal{F}_\ell^{\mathrm{cyc}}(X) : (A \setminus \{0_A\})(\mathcal{O}_L) \neq \varnothing\right\} \subseteq \mathcal{F}_{\mathcal{P},\ell}^{\mathrm{cyc}}(X),$$

where $\mathcal{F}_{\mathcal{P},\ell}^{\text{cyc}}(X)$ is defined in Proposition 4.1. By Proposition 4.1 (see also Remark (II) following that proposition), there are $c_1, c_2 > 0$ such that

$$\# \mathcal{F}_{\mathcal{P},\ell}^{\text{cyc}}(X) \sim c_1 \cdot \frac{X}{(\log X)^{1-\beta}}, \quad \# \mathcal{F}_{\ell}^{\text{cyc}}(X) \sim c_2 \cdot X$$

as $X \to \infty$, where

$$\beta = (\ell - 1)\alpha = \frac{\# H_\ell(A) - \# \mathcal{C}_\ell(A)}{\# H_\ell(A)}.$$

This proves the theorem.

Acknowledgements We would like to thank Ariyan Javanpeykar for useful discussions, and for bringing the Arithmetic Puncturing Problem to our attention. We are grateful to the referees for suggesting valuable improvements.

References

1. Anni, S., Lemos, P., Siksek, S.: Residual representations of semistable principally polarized abelian varieties. Res. Number Theory **2**, Art. No. 1 (2016)
2. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symb. Comput. **24**(3–4), 235–265 (1997)
3. Cao, Y., Liang, Y., Xu, F.: Arithmetic purity of strong approximation for homogeneous spaces. J. Math. Pures Appl. **132**, 334–368 (2019)
4. Cassels, J.W.S.: Local Fields. London Mathematical Society Student Texts, vol. 3, Cambridge University Press, Cambridge (1986)
5. Dieulefait, L.V.: Explicit determination of the images of the Galois representations attached to abelian surfaces with $\text{End}(A) = \mathbb{Z}$. Experiment. Math. **11**(4), 503–512 (2003)
6. Faltings, G.: Diophantine approximation on abelian varieties. Ann. Math. **133**(3), 549–576 (1991)
7. Freitas, N., Kraus, A., Siksek, S.: Local criteria for the unit equation and the asymptotic Fermat's last theorem. Proc. Natl. Acad. Sci. USA **118**(12), 2026449118 (2021)
8. Freitas, N., Kraus, A., Siksek, S.: The unit equation over cyclic number fields of prime degree. Algebra Number Theory **15**(10), 2647–2653 (2021)
9. Greenberg, R.: Introduction to Iwasawa theory for elliptic curves. In: Conrad, B., Rubin, K. (eds.) Arithmetic Algebraic Geometry (Park City, UT, 1999). IAS/Park City Mathematics Series, vol. 9, pp. 407–464. American Mathematical Society, Providence (2001). https://doi.org/10.1090/pcms/009
10. Hassett, B., Tschinkel, Yu.: Density of integral points on algebraic varieties. In: Peyre, E., Tschinkel, Yu. (eds.) Rational Points on Algebraic Varieties. Progress in Mathematics, vol. 199, pp. 169–197. Birkhäuser, Basel (2001). https://doi.org/10.1007/978-3-0348-8368-9_7
11. Iwasawa, K.: On Z_l-extensions of algebraic number fields. Ann. Math. **98**, 246–326 (1973)
12. Kresch, A., Tschinkel, Yu.: Integral points on punctured abelian surfaces. In: Fieker, C., Kohel, D.R. (eds.) Algorithmic Number Theory. Lecture Notes in Computer Science, pp. 198–204. Springer, Berlin (2002)

13. Liang, Y.: Approximation forte sur un produit de variétés abéliennes épointé en des points de torsion. Proc. Amer. Math. Soc. **148**(11), 4635–4642 (2020)
14. Mäki, S.: The conductor density of abelian number fields. J. London Math. Soc. **47**(1), 18–30 (1993)
15. Mazur, B., Rubin, K.: Ranks of twists of elliptic curves and Hilbert's tenth problem. Invent. Math. **181**(3), 541–575 (2010)
16. Milne, J.S.: Abelian varieties. In: Cornell, G., Silverman, J.H. (eds.) Arithmetic Geometry (Storrs, Conn., 1984), pp. 103–150. Springer, New York (1986)
17. Pollack, P.: The smallest inert prime in a cyclic number field of prime degree. Math. Res. Lett. **20**(1), 163–179 (2013)
18. Serre, J.-P.: Divisibilité de certaines fonctions arithmétiques. In: Séminaire Delange–Pisot–Poitou, 16e année (1974/75). Théorie des nombres, Fasc. 1, Exp. No. 20. Secrétariat Mathématique, Paris (1975). http://eudml.org/doc/110880
19. Serre, J.-P.: Lectures on the Mordell–Weil theorem. Aspects of Mathematics, E15. Friedr. Vieweg & Sohn, Braunschweig (1989). https://doi.org/10.1007/978-3-663-14060-3
20. Serre, J.-P.: Oeuvres/Collected papers. IV. 1985–1998. Springer Collected Works in Mathematics. Springer, Heidelberg (2013)
21. Silverman, J.H.: Integral points on abelian varieties. Invent. Math. **81**(2), 341–346 (1985)
22. Silverman, J.H.: The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics. Springer, New York (1986)
23. Silverman, J.H.: Advanced Topics in the Arithmetic of Elliptic Curves. Graduate Texts in Mathematics. Springer, New York (1994)
24. Tenenbaum, G.: Introduction to Analytic and Probabilistic Number Theory. Graduate Studies in Mathematics, vol. 163. 3rd edn. American Mathematical Society, Providence (2015). https://doi.org/10.1090/gsm/163
25. The LMFDB Collaboration. The L-functions and modular forms database (2021). http://www.lmfdb.org. [Online; accessed 6 April 2021]
26. Urazbaev, B.M.: On the density of distribution of cyclic fields of prime degree. Izvestiya Akad. Nauk Kazah. SSR Ser. Mat. Meh. **5**(62), 37–52 (1951)
27. Vojta, P.: Integral points on subvarieties of semiabelian varieties. II. Amer. J. Math. **121**(2), 283–313 (1999)
28. Washington, L.C.: Introduction to Cyclotomic Fields. Graduate Texts in Mathematics. Springer, New York (1997)
29. Wright, D.J.: Distribution of discriminants of abelian extensions. Proc. London Math. Soc. **58**(1), 17–50 (1989)
30. Zarhin, Yu.: n-th root of unity in n-th division field of abelian variety? MathOverflow. https://mathoverflow.net/q/208405 (version: 2015-06-04)