Math. Res. Lett. **14** (2007), *no.* 5, 731–743

ABELIAN POINTS ON ALGEBRAIC VARIETIES

Pete L. Clark

Abstract. We attempt to determine which classes of algebraic varieties over $\mathbb{Q}$ must have points in some abelian extension of $\mathbb{Q}$. We give: (i) for every odd $d > 1$, an explicit family of degree d, dimension $d-2$ diagonal hypersurfaces without $\mathbb{Q}^{\mathrm{ab}}$-points, (ii) for every number field K, a genus one curve $C_{/\mathbb{Q}}$ with no K^{ab}-points, and (iii) for every $g \geq 4$ an algebraic curve $C_{/\mathbb{Q}}$ of genus g with no $\mathbb{Q}^{\mathrm{ab}}$-points. In an appendix, we discuss varieties over $\mathbb{Q}((t))$, obtaining in particular a curve of genus 3 without $\mathbb{Q}((t))^{\mathrm{ab}}$-points.

Convention: When we speak of a *curve*, a *surface* or a *variety* over a field K, we shall require it to be nonsingular, projective and (most important of all for what follows) geometrically irreducible. However, by a *hypersurface* we mean the closed subscheme of projective space defined by any homogeneous polynomial.

1. Introduction

1.1. A theorem of Frey. In [6], G. Frey demonstrated the existence of an algebraic variety $V_{/\mathbb{Q}}$ with no points rational over the maximal abelian extension $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}$ (or "without abelian points.") His argument uses a mixture of elliptic curve theory and valuation theory;[1] from it, one can deduce the existence of an abelian variety $A_{/\mathbb{Q}}$ and a principal homogeneous space $V_{/\mathbb{Q}}$ for A such that $V(\mathbb{Q}^{\mathrm{ab}}) = \emptyset$.

1.2. Statements of the main results. The purpose of this paper is to take a closer look at algebraic varieties – especially curves – without abelian points. Let us first give an "optimally" concrete and simple example.

Theorem 1. *("Easy Theorem," v. I)*
Let $p \equiv -1 \pmod 3$ be a prime, and let $a,\ b,\ c \in \mathbb{Z}$, $(abc, p) = 1$. The curve

$$aX^3 + bpY^3 + cp^2Z^3 = 0 \qquad (1)$$

has no $\mathbb{Q}_p^{\mathrm{ab}}$-points.

Proof: We observe first that C has no $\mathbb{Q}_p$-rational points. For, if not, we would have a solution $(x, y, z) \in \mathbb{Z}_p^3$ with $\min(\mathrm{ord}_p(x),\ \mathrm{ord}_p(y),\ \mathrm{ord}_p(z)) = 0$, and this is visibly impossible: looking at the equation we see that p must divide first x, then y, then finally z. Moreover, if $K/\mathbb{Q}_p$ is any finite extension with uniformizer π and ramification index $e(K/\mathbb{Q}_p)$ prime to 3, then running through the above argument with ord_π in place of ord_p shows that C has no K-rational points.

But now suppose that there exists a solution in the ring of integers of $\mathbb{Q}_p(\mu_N)$ for some positive integer N. Write $N = M \cdot p^i$ with $(M, p) = 1$. We have

Received by the editors May 16, 2006. Revised February 27, 2007.

[1]One finds a purely algebraic proof in [5].

$e(\mathbb{Q}_p(\mu_N)/\mathbb{Q}_p) = \varphi(p^i) = p^{i-1}(p-1)$, which is, by our assumption on p, prime to 3. The proof is completed by recalling that the maximal abelian extension of $\mathbb{Q}_p$ is obtained by adjoining all roots of unity [18, Thm. XIV.2].

For "most" number fields K, we can choose p such that all the curves (1) fail to have K^{ab}-rational points. More precisely:

Corollary 2. *Let K be a number field whose Galois closure does* not *contain $\mathbb{Q}(\mu_3)$. Then there exists a prime p such that the curves (1) have no K^{ab}-rational points.*

Proof: Thanks to our assumption on K, Cebotarev's density theorem guarantees the existence of infinitely many primes $p \equiv -1 \pmod 3$ such that p splits completely in K. We then have an embedding $K^{\mathrm{ab}} \hookrightarrow \mathbb{Q}_p^{\mathrm{ab}}$, and by Theorem 1 we conclude that $aX^3 + pbY^3 + p^2cZ^2 = 0$ has no K^{ab}-rational points.

In fact, with rather more work, we can (and shall) prove the following result.

Theorem 3. *For each number field K, there is a genus one curve $C_{/\mathbb{Q}}$ with $C(K^{\mathrm{ab}}) = \emptyset$.*

Next we wish to determine the genera g for which some genus g curve $C_{/\mathbb{Q}}$ has $C(\mathbb{Q}^{\mathrm{ab}}) = \emptyset$. Since quadratic extensions are abelian, a curve $C_{/\mathbb{Q}}$ which admits a degree 2 morphism to a curve Y with $Y(\mathbb{Q}) \neq \emptyset$ certainly has abelian points. Taking $Y = \mathbb{P}^1$ we see that there are abelian points on all hyperelliptic curves – by a hyperelliptic curve, we mean a curve of any genus admitting a degree two map to $\mathbb{P}^1$, and not merely to a conic – and in particular on all curves of genus 0 or 2.

In fact we can get further mileage out of our easy Theorem 1: the same proof shows the following:

Theorem 4. *("Easy Theorem," v. II)*
Let p be a prime and $d > 1$ an integer which is prime to $p(p-1)$. Then

$$\sum_{i=0}^{d-1} p^i X_i^d = 0 \tag{2}$$

has no points over $\mathbb{Q}_p^{\mathrm{ab}}$.

We urge the reader to see for herself how the proof (alas!) breaks down when $(d, p(p-1)) > 1$, so in particular for every prime p when d is even. Conversely, for any *odd* $d \geq 3$, choose, by Dirichlet's theorem, a prime p with $p \equiv -1 \pmod d$. Then Theorem 4 applies to give a degree d hypersurface of Calabi-Yau type without $\mathbb{Q}^{\mathrm{ab}}$-points. Intersecting with a general 2-plane – and applying Bertini's theorem; cf. the proof of Corollary 23 – we conclude:

Corollary 5. *For odd $d \geq 3$, there is a degree d plane curve $C_{/\mathbb{Q}}$ with $C(\mathbb{Q}^{\mathrm{ab}}) = \emptyset$.*

By quite different methods we will prove the following result.

Theorem 6. *For all $g \geq 4$, there exists $C_{/\mathbb{Q}}$ of genus g and such that $C(\mathbb{Q}^{\mathrm{ab}}) = \emptyset$.*

Conspicuously missing is the case of $g = 3$. Equivalently, we wonder:

Question 7. *Must a nonsingular plane quartic curve $C_{/\mathbb{Q}}$ have an abelian point?*

1.3. Some perspective on the proofs. Suppose more generally that L/K is a field extension, and we are interested in generating a large supply of varieties $V_{/K}$ with $V(L) = \emptyset$. For a particular concretely given variety $V_{/K}$, the question may be prohibitively difficult (even $L = K = \mathbb{Q}$ may be algorithmically impossible). Indeed, this paper sprung out of a question posed to me by **D. Jetchev** of U.C. Berkeley: is there an abelian cubic field, or any abelian number field L, over which Selmer's cubic curve

$$C : 3X^3 + 4Y^3 + 5Z^3 = 0 \tag{3}$$

has L-rational points? Because Selmer's curve has points everywhere locally (but no $\mathbb{Q}$-points) I could make no progress, and I pass it along to you as a very interesting open problem.[2] On the other hand the cubic curve $2X^3 + 4Y^3 + 5Z^3 = 0$, which is in some (rather silly) sense "close" to Selmer's cubic, does not have any $\mathbb{Q}^{\mathrm{ab}}$-points, a special case of Theorem 1!

Evidently then there are some curves (and hypersurfaces) that are "rigged" to have no abelian points, even over a suitable completion. So the first step of our strategy is to find such rigged varieties, even if they are geometrically of a very special form. Over $\mathbb{Q}$ the rigging seems to take place in Kodaira dimension zero: our examples all involve Calabi-Yau hypersurfaces and torsors under abelian varieties. In the latter case the machinery of Galois cohomology gives especially good control. In fact, I was led to the cubic curves (1) by Galois cohomological considerations, although for simplicity these are not reproduced here.[3]

The second step of our strategy is to extend the class of varieties using the following evergreen observation: if $V_{/K}$ has no L-rational points, then neither does any variety $W_{/K}$ which admits a morphism $f : W \to V$.[4] As a special case, the property of having no L-rational points passes from V to any subvariety W of V (as in Corollary 5). At the other extreme we can take f to be a branched covering: we will prove Theorem 6 using degree two coverings of a genus one curve X. However, although geometrically any genus one curve admits degree two coverings by curves of all genera $g \geq 2$, this is not true for genus one curves X without abelian points: the *index* $i(X)$ of X must satisfy $2 < i(X) \mid 2g - 2$. Until recently it was not known whether there were any genus one curves over $\mathbb{Q}$ of each given index, but the methods of [2] allow for a reasonably flexible construction of cohomology classes of most indices in $H^1(\mathbb{Q}, E)$ for an elliptic curve $E_{/\mathbb{Q}}$ satisfying suitable hypotheses. Thanks to work of Mazur-Rubin, the Jacobian of Selmer's curve satisfies these hypotheses, and we construct the curves of Theorem 6 as quadratic covers of twists of C. The proof of Theorem 3 is of a much more *ad hoc* nature and uses difficult theorems of Gross-Zagier-Kolyvagin and Ono-Skinner. Whether such pyrotechnics are really necessary remains to be seen. The proofs of these results occupy §3.

A commonality between the "easy" and Galois cohomological approaches to rigged varieties is their ultimate reduction to local results: every theorem of the form $V(K^{\mathrm{ab}}) = \emptyset$ for V a variety over a number field K is obtained by showing that

[2](added in proof): This problem has recently been solved by Ronald van Luijk: there *is* an abelian cubic splitting field.

[3]Whether the hypersurfaces (2) can also be explained cohomologically I do not know.

[4]Note that this strategy is no help in producing examples of negative Kodaira dimension. We return to this issue in §4.

$V(K_v^{\mathrm{ab}}) = \emptyset$ for some place v of K. So we set the stage in §2 with a local analysis. The key result is that for every p-adic field K, there is a genus one curve $C_{/K}$ with $C(K^{\mathrm{ab}}) = \emptyset$ (Theorem 11).

1.4. Conjectures and Open Problems. Although Question 7 is the most conspicuous problem left open by this work, there are many others. In particular, although our motivation for studying abelian points on varieties was, essentially, "why not?" these and similar questions (for other infinite extensions $L/\mathbb{Q}$) are deeply connected to other results and conjectures in arithmetic geometry. Some of these further problems are explored in §4.

1.5. More general fields. After seeing an early draft of this paper, B. Poonen commented that it might be of interest to investigate the existence of abelian points on varieties over arbitrary fields, as is done in [17] for solvable points. In the Appendix we carry out some of these explorations. Especially, taking $\mathbb{F} = \mathbb{Q}((t))$ we obtain curves of genus 3 and geometrically rational surfaces without abelian points.

Acknowledgements: The first draft of this paper was written during a postdoctoral fellowship I held at MSRI during the 2006 Rational and Integral Points (RIP) program. It is very much a product of that exciting climate, and in particular I benefitted greatly from conversations with Bjorn Poonen, Jean-Louis Colliot-Thélène, Mirela Ciperiani and Dimitar Jetchev. I reserve especially hearty thanks for the fantastic referee. Apart from suggesting many expository improvements, s/he spotted a significant simplification of the proof of Theorem 11 and suggested a strengthening of (what is now) Theorem 4.

2. Local fields

We identify principal homogeneous spaces V for an abelian variety $A_{/K}$ with Galois cohomology classes $\eta \in H^1(K, A)$. It is thus natural to speak of a field extension L/K such that $V(L) \neq \emptyset$ as a *splitting field* for V (or for the corresponding class η).

For $\eta \in H^1(K, A)$, its *period* is the order of η as an element of the torsion abelian group $H^1(K, A)$ and its *index* is the greatest common divisor of all $[L : K]$ for L/K a splitting field for η. When $A = E$ has dimension one, the index of η is equal to the least positive integer which is the degree of a K-rational divisor on the corresponding genus one curve C. To any K-rational divisor of degree $n \geq 3$ there corresponds a nondegenerate degree n embedding of C into $\mathbb{P}^{n-1}$ and conversely (up to linear equivalence of divisors and automorphisms of projective space); in particular, the curves of index 3 are precisely the plane cubic curves without rational points.

In this section the ground field K is a finite extension of $\mathbb{Q}_p$, with valuation ring R and residue field $\mathbb{F}_q$, $q = p^a$. Let r be the cardinality of the group of roots of unity in K, so $q - 1 \mid r$ and $\frac{r}{q-1}$ is a power of p.

Our point of departure is the following result:

Theorem 8. *(Lang-Tate,* [11]*) Let $A_{/K}$ be an abelian variety with good reduction, and let V be a principal homogeneous space for A whose order, n, is prime to p. For*

a finite field extension L/K, the following are equivalent:
(i) $V(L) \neq \emptyset$.
(ii) The ramification index $e(L/K)$ *is divisible by* n.

From this we deduce the following result, a sharpening of the example of [3, §2.3].

Proposition 9. *Let V be a principal homogeneous space of an abelian variety $A_{/K}$ with good reduction, whose period n is prime to p and does not divide $r = \#\mu(K)$. Then $V(K^{\mathrm{ab}}) = \emptyset$.*

Proof: Suppose on the contrary that L/K is an abelian extension with $V(L) \neq \emptyset$. We may decompose L/K into a tower of extensions

$$K = F_0 \subset F_1 \subset F_2 \subset F_3 = L$$

such that F_1/F_0 is unramified, F_2/F_1 is totally ramified and of degree prime to p, and F_3/F_2 is totally ramified of degree a power of p (e.g. [18]). Put $d = [F_2 : F_1]$.

We work with the corresponding Galois cohomology class $\eta \in H^1(K, A)[n]$, our assumption being that $\eta|_{F_3} = 0$. Since $[F_3 : F_2]$ is prime to n, we have $\eta|_{F_2} = 0$ [3, Prop. 11]. By Theorem 8, we have that $n \mid d$, and by the known structure of totally tamely ramified Galois extensions of local fields [18], there exists a uniformizer π of F_1 such that $F_2 = F_1[X]/(X^d - \pi)$. Since L/K is abelian, so is F_2/F_0, which implies that $\mu_d \subset F_0$. In other words, $n \mid d \mid r$, a contradiction.

It is thus in our interest to give conditions for the existence of classes $\eta \in H^1(K, A)$ of a given order n (prime to p and not dividing r). To ease the notation in the proof of the next result, we write B for the dual abelian variety $A^\vee$. (Of course $B \cong A$ when A is principally polarized, and in particular for elliptic curves.)

Lemma 10. *Let $\tilde{A}_{/\mathbb{F}_q}$ be the good reduction of $A_{/K}$. If $\tilde{A}(\mathbb{F}_q)$ has an element of order n, with $(n, p) = 1$, then there exists $\eta \in H^1(K, B)$ of order n.*

Proof: By a seminal theorem of Tate [21], the discrete abelian group $H^1(K, B)$ and the profinite abelian group $A(K)$ are in Pontrjagin duality. It follows that the finite abelian groups $H^1(K, B)[n]$ and $A(K)/nA(K)$ are in duality and hence are isomorphic. Reduction modulo the maximal ideal of K gives an epimorphism $\mathcal{R} : A(K) \to \tilde{A}(\mathbb{F}_q)$, whose kernel K is uniquely n-divisible. So $\mathcal{R}$ induces an isomorphism $A(K)/nA(K) \xrightarrow{\sim} \tilde{A}(\mathbb{F}_q)/n\tilde{A}(\mathbb{F}_q)$, and the result follows.

Theorem 11. *There is a genus one curve $C_{/K}$ with $C(K^{\mathrm{ab}}) = \emptyset$.*

Proof: Assume for the moment the following

Claim. *There exists a prime ℓ such that*
• *ℓ is prime to $q(q-1)$.*
• *There is an elliptic curve $E_{/\mathbb{F}_q}$ with $\ell \mid \#E(\mathbb{F}_q)$.*

Then: let $\tilde{E}$ be any lift of E to an elliptic curve over K (e.g., choose representatives in R of the coefficients of a Weierstrass equation of E). By Lemma 10 there exists a class $\eta \in H^1(K, \tilde{E})$ of order ℓ, and since ℓ is prime to $(q-1)q$ it does not divide r. So by Proposition 9, the corresponding genus one curve $C_{/K}$ has $C(K^{\mathrm{ab}}) = \emptyset$.

It remains to prove the claim. Let us first recall the following cases of the Deuring-Waterhouse classification of the integers N which are $\#E(\mathbb{F}_q)$ for some elliptic curve $E_{/\mathbb{F}_q}$ [22, Theorem 4.1]: there exists such an N of the form $q+1-t$ when t is an integer with $|t| \leq 2\sqrt{q}$ satisfying *either* of the following additional hypotheses: (i) $(t,p)=1$; or (ii) $p \not\equiv 1 \mod 4$ and $t=0$.
Define a positive integer N as follows:

Case 1 ($p=2$): $N=q+1$.
Case 2 ($p=3$): $N=q+2$.
Case 3 ($p \geq 5$): $N=q-2$.

Now in all cases we we may take ℓ to be any prime divisor of N. This establishes the Claim and completes the proof of Theorem 11.

Remark: When A has split purely toric reduction, every class $\eta \in H^1(K,A)$ has a unique minimal splitting extension L_η, which is abelian over K [7], [3, §3.1].

3. Number fields

3.1. Curves of genus one.

Theorem 12. *Let $E_{/\mathbb{Q}}$ be the Jacobian of Selmer's cubic curve $C: 3X^3+4Y^3+5Z^3 = 0$ and let ℓ be either 4 or an odd prime. There exists a class $\eta \in H^1(\mathbb{Q},E)$ such that:*
(i) η has period and index equal to ℓ.
(ii) η does not have an abelian splitting field.

Proof: We note for future reference that $E(\mathbb{Q})=0$, $Ш(\mathbb{Q},E) \cong (\mathbb{Z}/3\mathbb{Z})^2$ and $j(E)=0$, so E has CM by the maximal order in $\mathbb{Q}(\sqrt{-3})$ [13].

Suppose first that $\ell \geq 5$. Then by Poitou-Tate duality, a strong form of the local-global principle holds in $H^1(\mathbb{Q},E)[\ell^\infty]$, namely the natural map

$$H^1(\mathbb{Q},E)[\ell^\infty] \to \bigoplus_p H^1(\mathbb{Q}_p,E)[\ell^\infty] \tag{4}$$

is an isomorphism [15, I.6.26(b)]. (Note that $H^1(\mathbb{R},E)[\ell^\infty]=0$ since ℓ is odd. In any case, $H^1(\mathbb{R},E)=0$ for this E.) There exist infinitely many primes p such that:

(i) $p>3$;
(ii) $p \equiv -1 \pmod 3$;
(iii) $p \equiv -1 \pmod \ell$.
(iv) E has good reduction mod p.

Fix one such prime p. Condition (ii) means that p is nonsplit in the CM field $\mathbb{Q}(\sqrt{-3})$, so by a well-known criterion of Deuring, E has supersingular reduction modulo p (or see [20, Example V.4.4]), so (using (i)), $\#E(\mathbb{F}_p)=p+1$ and hence, by (iii), $\ell \mid \#E(\mathbb{F}_p)$. By Lemma 10, there exists $\eta_p \in H^1(\mathbb{Q}_p,E)$ of order ℓ. Because the map of (4) is an isomorphism, there exists a unique class $\eta \in H^1(\mathbb{Q},E)[\ell]$ restricting at p to η_p and having trivial restriction at all other primes. By [2, Prop. 6], we conclude that η has period and index equal to ℓ. Since $p \equiv -1 \pmod \ell$, evidently ℓ does not divide

$p - 1 = \#\mu(\mathbb{Q}_p)$, so by Proposition 9, η_p (and *a fortiori* η itself) has no abelian splitting field.

The case $\ell = 3$ is in fact covered by Theorem 1. To see this, recall that an equation for the Jacobian of $aX^3 + bY^3 + cZ^3 = 0$ is $X^3 + Y^3 + abcZ^3 = 0$ (this is "classical"; see e.g. [1] for a careful modern treatment). In particular $X^3 + Y^3 + 60Z^3 = 0$ is a defining equation for E; so for any prime $p \equiv -1 \pmod 3$, $X^3 + pY^2 + 60p^2Z^2$ can be endowed with the structure of a principal homogeneous space over E. Theorem 1 implies that any such curve has no abelian splitting field; in particular it has no rational points hence has index and period equal to 3.

For $\ell = 4$, take $p = 11$ (so $4 \not| \ p-1$); one checks easily that $\tilde{E}(\mathbb{F}_{11}) \cong \mathbb{Z}/12\mathbb{Z}$.

3.2. Curves of genus $g \geq 4$. We will reduce to the case of curves of genus one via the following result, a version of which was suggested to me by B. Poonen *en route* to Sabino Canyon in 2003.[5]

Proposition 13. *Let K be an infinite field of characteristic different from 2, and let $Y_{/K}$ be a genus one curve of index $n > 1$. For any positive integer k, there exists a curve $X_{/K}$ of genus $nk + 1$ and a degree two covering $X \to Y$ defined over K.*

Proof: By definition of the index there exists a K-irreducible divisor D_0 on Y of degree n. By the Riemann-Roch theorem, the set $L(|D_0|)$ of effective divisors linearly equivalent to D_0 forms a projective space over K of dimension $n - 1 > 0$. Since K is infinite, we may choose, for any positive integer k, $2k$ distinct elements of $L(|D_0|)$, say, $D_1, \ldots, D_{2k}$. Consider the divisor

$$D = \sum_{i=1}^{k} (D_i - D_{i+k}).$$

First, D is linearly equivalent to zero, so is the divisor of a function $f \in K(Y)$. Second, the support of D has cardinality equal to $2k$: indeed, this follows from the transitivity of the Galois action on every effective K-rational divisor of degree k: if $P \in \operatorname{supp}(D_i) \cap \operatorname{supp}(D_j)$, then D_i and D_j are each the complete $\mathfrak{g}_K$-orbit of P, so are equal. Thus the extension of function fields $K(Y)(\sqrt{f})/K(Y)$ corresponds to a degree 2 cover $X \to Y$ with $2kn$ simple branch points. By the Riemann-Hurwitz formula, X has genus $kn + 1$.

Let us now prove Theorem 6. A positive integer $g \geq 4$ may be written as $k\ell + 1$ with $k \in \mathbb{Z}^+$ and ℓ either an odd prime or 4. By Theorem 12 there exists a genus one curve $Y_{/\mathbb{Q}}$ of index ℓ without abelian points. Applying Proposition 13 with $n = \ell$, we get a curve X of genus g together with a degree two map $X \to Y$. Since Y has no abelian points, neither does X.

3.3. The proof of Theorem 3. Let $n = [K : \mathbb{Q}]$. Let $\ell > 7$ and p be distinct primes, each unramified in K, such that ℓ does not divide $p^a - 1$ for any $1 \leq a \leq n$; then no completion of K at a prime over p has a rational ℓth root of unity. **Suppose** $\tilde{E}_{/\mathbb{F}_p}$ is an elliptic curve with an $\mathbb{F}_p$-rational point of order ℓ. Lift $\tilde{E}$ to an elliptic

[5]This same idea was later broached to Poonen's student S. Sharif, whose 2006 Berkeley thesis employs it as the jumping-off point for a complete determination of the possible values of a period and index for a genus g curve over a p-adic field. The result is also used in [4].

curve $E_{/\mathbb{Q}}$. By a theorem of Ono-Skinner [16], there exists an elliptic curve $E'_{/\mathbb{Q}}$ such that:

(i) $E'_{/\mathbb{Q}_p} \cong E_{/\mathbb{Q}_p}$ (in particular $j(E) = j(E')$);
(ii) E' has analytic rank zero.

(More precisely, E' is the twist of E by a quadratic Dirichlet character χ with $\chi(p) = 1$.) By the results of Gross-Zagier and Kolyvagin, it follows that $E'(\mathbb{Q})$ and $Ш(\mathbb{Q}, E)$ are both finite. Moreover, since $\ell > 7$, Mazur's theorem on rational torsion points on elliptic curves [13] gives $E'(\mathbb{Q}) \otimes \mathbb{Z}_\ell = 0$. Now the Poitou-Tate global duality theorem applies to show that the natural map

$$H^1(\mathbb{Q}, E')[\ell^\infty] \to \bigoplus_p H^1(\mathbb{Q}_p, E')[\ell^\infty]$$

is a surjection. In particular, there exists a class $\eta \in H^1(\mathbb{Q}, E')[\ell^\infty]$ whose local restriction η_p has order ℓ. Since $K/\mathbb{Q}$ is unramified at p, by Theorem 8 $\eta|_K$ has exact order ℓ, and by the same arguments as above does not split over any abelian extension of the completion of K at any prime over p.

It remains to show that, for some choices of ℓ and p as above, there exists $\tilde{E}_{/\mathbb{F}_p}$ with a point of order ℓ. For this, we consider primes $p > n + 1$. Another special case of the Deuring-Waterhouse classification [22, Theorem 4.1] gives that for any integer $A \in (p + 1 - 2\sqrt{p},\ p + 1 + 2\sqrt{p})$, there exists $E_{/\mathbb{F}_p}$ with $\#E(\mathbb{F}_p) = A$. In particular, for every $\ell < \sqrt{p}$, there exists $E_{/\mathbb{F}_p}$ with an element of order ℓ. There are at most n primes $\ell < \sqrt{p}$ whose order, as elements of $\mathbb{F}_p^\times$, is at most n, so when p is sufficiently large compared to n there are many primes ℓ such that there exists $E_{/\mathbb{F}_p}$ with elements of order ℓ. This completes the proof of the theorem.

4. Open Problems

4.1. Conjectural strengthenings.

Conjecture 14. *Let $L \supset K$ be number fields and $A_{/K}$ an abelian variety.*
a) There is a torsor $V_{/K}$ under A with $V(L^{\mathrm{ab}}) = \emptyset$.
b) For all $d \geq 3$, there is a degree d plane curve $C_{/K}$ such that $C(L^{\mathrm{ab}}) = \emptyset$.
c) For all $g \geq 3$, there is a curve $C_{/K}$ of genus g such that $C(L^{\mathrm{ab}}) = \emptyset$.

4.2. Negative Kodaira dimension. As remarked in §1.3, we have no examples in negative Kodaira dimension of varieties $V_{/\mathbb{Q}}$ with $V(\mathbb{Q}^{\mathrm{ab}}) = \emptyset$. If such examples exist, probably they lie very deep, and would be of significant interest. Indeed:

(i) Emil Artin asked whether a Fano hypersurface (i.e., the zero locus of a degree d homogeneous polynomial in at least $d + 1$ variables) defined over $\mathbb{Q}^{\mathrm{ab}}$ must have a rational point. By a celebrated theorem of Lang [10], such hypersurfaces have points everywhere locally.

(ii) By work of Brauer and Birch, the existence of quadratic points is known for "sufficiently Fano" hypersurfaces: for every fixed d, there exists $n = n(d)$ such that a degree d form in n variables over $\mathbb{Q}$ has a nontrivial solution in (e.g.) $\mathbb{Q}(\sqrt{-1})$.

(iii) Kanevsky has shown [9] that if $V_{/K}$ is a cubic surface over a number field K

such that for all finite extensions L/K, the Brauer-Manin obstruction to the existence of L-rational points on $V_{/L}$ is the only one (as is widely believed to be the case), then $V(K^{\mathrm{ab}}) \neq \emptyset$.

4.3. Varieties *with* abelian points. One can ask for nontrivial examples of varieties with abelian points; let us say, not coming from a quadratic covering of a variety with $\mathbb{Q}$-points. The best example I know is that of Severi-Brauer varieties (varieties $V_{/\mathbb{Q}}$ such that $V_{/\overline{\mathbb{Q}}} \cong \mathbb{P}^N_{/\overline{\mathbb{Q}}}$): there are always abelian points, but, in dimension at least two, usually not quadratic points. Indeed, the Brauer-Hasse-Noether theorem says that every element of the Brauer group of a number field is given by a cyclic algebra.[6]

Problem 15. *For all positive integers n (or even for infinitely many n), exhibit a genus one curve $C_{/\mathbb{Q}}$ of index n and such that $C(\mathbb{Q}^{\mathrm{ab}}) \neq \emptyset$.*

Perhaps the solution to Problem 15 will involve Iwasawa theory.

4.4. Varieties with local points. In the same vein as Jetchev's question, we ask:

Question 16. *Fix a positive integer n. Does every locally trivial genus one curve of index n defined over a number field have an abelian point?*

4.5. Solvable points. We were also motivated by work in progress of M. Ciperiani and A. Wiles, who study *solvable* points on curves of genus one. They are able to show that a genus one curve $C_{/\mathbb{Q}}$ which is locally trivial and with semistable Jacobian has a solvable point.

Using the solvability of the absolute Galois groups of $\mathbb{Q}_p$ and $\mathbb{R}$, it is easy to see that for every variety V over a number field K, there is a solvable extension L/K such that $V_{/L}$ has points everywhere locally. Thus, an affirmative answer to Question 16 for all n would imply the existence of solvable points on all curves of genus one.

4.6. Metabelian points. Note that in Section 2, all our examples of principal homogeneous spaces over $\mathbb{Q}_p$ without abelian points have points over the maximal abelian extension of $\mathbb{Q}_p^{\mathrm{ab}}$, i.e., over a **metabelian** extension of $\mathbb{Q}_p$. It was suggested to me a few years ago by B. Mazur that every genus one curve over $\mathbb{Q}$ should have metabelian points. This remains open even over $\mathbb{Q}_p$, although special cases follow from results of Lang-Tate [11] and Lichtenbaum [12].

Appendix: varieties over $\mathbb{Q}((t))$

A somewhat different perspective would be to fix a "type" of algebraic varieties (e.g., curves of a given genus g, or hypersurfaces of degree d in $\mathbb{P}^N$) and ask whether for *every* field F, a variety $V_{/F}$ of this type must have points in the maximal abelian extension of F. With "abelian" replaced by "solvable," this is the setting of recent work of A. Pál [17]. In this appendix we will show that, with a suitable choice of F, there are additional classes of F-varieties without F^{ab}-points. As our approach is far from exhaustive in any event, let us simplify matters by imposing throughout this appendix the running assumption that all our fields are perfect.

[6] Or see [19, § II.3.3, Prop. 9] for a more elementary argument showing that $\mathrm{Br}(\mathbb{Q}^{\mathrm{ab}}) = 0$.

A convenient choice of field is $\mathbb{F} = \mathbb{Q}((t))$. The absolute Galois group $\mathfrak{g}_{\mathbb{F}}$ of $\mathbb{F}$ lies in a split exact sequence

$$1 \to \hat{\mathbb{Z}} \to \mathfrak{g}_{\mathbb{F}} \to \mathfrak{g}_{\mathbb{Q}} \to 1$$

where $\mathfrak{g}_{\mathbb{Q}}$ acts on $\hat{\mathbb{Z}}$ by the cyclotomic character. Thus the maximal abelian extension of $\mathbb{F}$ is generated by the roots of unity together with $t^{\frac{1}{2}}$. The field $\mathbb{F}(\mu_\infty, t^{\frac{1}{2}})$ is Henselian with respect to the discrete valuation $\frac{\mathrm{ord}_t}{2}$. We will work instead with its completion $\mathbb{K} := \mathbb{Q}^{\mathrm{ab}}((t^{\frac{1}{2}}))$. Since $\mathbb{K}$ contains $\mathbb{F}^{\mathrm{ab}}$, to say of a variety $V_{/\mathbb{F}}$ that V has no $\mathbb{K}$-points is at least as strong as saying it has no $\mathbb{F}^{\mathrm{ab}}$-points.

Proposition 17. *Every Severi-Brauer variety $V_{/\mathbb{F}}$ has an abelian point, but there exist Severi-Brauer varieties $V_{/\mathbb{K}}$ without rational points.*

Proof: This may be viewed as a question about the Brauer groups $\mathrm{Br}(\mathbb{F})$ and $\mathrm{Br}(\mathbb{K})$ (e.g. [18, §X.6]). For any complete, discretely valued field F with perfect residue field f, there is an exact sequence

$$0 \to \operatorname{Br} f \to \operatorname{Br} F \xrightarrow{c} X(\mathfrak{g}_f) \to 0,$$

where the last term is the character group of the Galois group of the residue field [18, Theorem X.3.2]. Consider first the case of $\mathbb{F} = \mathbb{Q}((t))$, so $f = \mathbb{Q}$. Then, for $\alpha \in \operatorname{Br}\mathbb{F}$ we can split the character $c(\alpha)$ via a unique unramified abelian extension $L/\mathbb{F}$ with (abelian) residue extension $l/\mathbb{Q}$. By the exact sequence, $\alpha|_L \in \mathrm{Br}(l)$. Now every element of the Brauer group of a number field can be split by a cyclotomic extension, so overall we get that $\mathrm{Br}(\mathbb{Q}((t))) = \mathrm{Br}(\mathbb{Q}^{\mathrm{ab}}((t))/\mathbb{Q}((t)))$, giving the first statement of the proposition.

On the other hand, $\mathbb{K} = \mathbb{Q}^{\mathrm{ab}}((t^{1/2})) \cong \mathbb{Q}^{\mathrm{ab}}((t))$ is again a local field, whose residue field $\mathbb{Q}^{\mathrm{ab}}$ has trivial Brauer group but highly nontrivial character group. For example, the quaternion algebra $\langle \sqrt{2}, t^{\frac{1}{2}} \rangle$ is nontrivial in $\mathrm{Br}(\mathbb{K})$.

The following result stands in stark contrast with the discussion of §4.2.

Corollary 18. *There exists a geometrically rational 4-fold $V_{/\mathbb{F}}$ with $V(\mathbb{K}) = \emptyset$.*

Proof: The quaternion algebra $\langle \sqrt{2},\ t^{\frac{1}{2}} \rangle$ defined over $\mathbb{F}' = \mathbb{F}(\sqrt{2}, t^{\frac{1}{2}})$ is nonsplit over $\mathbb{K}$; it corresponds to a conic $C_{/\mathbb{F}'}$ with $C(\mathbb{K}) = \emptyset$. Restriction of scalars from $\mathbb{F}'$ to $\mathbb{F}$ gives a fourfold $V_{/\mathbb{F}}$ such that $V_{/\overline{\mathbb{F}}} \cong (\mathbb{P}^1)^4$ and $V(\mathbb{K}) = C(\mathbb{F}' \otimes_{\mathbb{F}} \mathbb{K}) = C(\prod_{i=1}^4 \mathbb{K}) = C(\mathbb{K})^4 = \emptyset$.

A theorem of Merkurjev-Suslin [14] implies that Severi-Brauer varieties over a perfect field have metabelian points. Surprisingly, the following seems to be open.

Question 19. *Does every Severi-Brauer variety have abelian points?*

Recall the **norm form** $N(L/K)$ associated to a separable algebra L/K of (finite) dimension d: choosing a K-basis $\alpha = (\alpha_1, \ldots, \alpha_d)$ of L, the map

$$N_\alpha : K^d \to K,\ (x_1, \ldots, x_d) \mapsto N(\sum_{i=1}^d x_i \alpha_i)$$

"evaluated at a generic point $x_1, \ldots, x_d$" of K^d yields a homogeneous degree d polynomial, which determines a hypersurface N_α in $\mathbb{P}^{d-1}$. Since any other basis α' is

$GL_d(K)$-conjugate to α, the norm hypersurface is well-determined up to an automorphism of projective space, and in particular gives a projective K-scheme (albeit not a variety according to our conventions).

A homogeneous K-form $f(X_1, \ldots, X_d)$ is *isotropic* if there are $(x_1, \ldots, x_d)$, not all zero, with $f(x_1, \ldots, x_d) = 0$; otherwise it is *anisotropic*.

If M/K is a finite field extension, then $N(L/K)_{/M}$ is the norm form for $L \otimes_K M/M$, and is anisotropic if and only if $L \otimes_K M$ is a field. In other words:

Lemma 20. *Let M/K be a finite field extension. Then the norm form $N = N(L/K)$ is anistropic over M if and only if M and L are linearly disjoint over K.*

Let us say that a finite extension M/K is *anabelian* if the maximal abelian subextension of M/K is K itself. The name comes from the fact that an anabelian extension is linearly disjoint from any abelian extension L/K. In particular, if $L = K[X]/(f)$ where f has degree $d \geq 3$ and Galois group S_d, then L/K is anabelian: such an extension does not even admit a nontrivial sub-Galois extension.

Note that the norm form $N(L/K)$ of a nontrivial field extension is geometrically reducible. Indeed, over the Galois closure of L/K, with a suitable choice of basis N becomes $N(X_1, \ldots, X_d) = X_1 \cdots X_d$. The corresponding closed subscheme of $\mathbb{P}^{d-1}$ is of dimension $d-2$ and has as its singular locus a finite union of linear subspaces of dimension $d-3$.

Proposition 21. *Fix a positive integer $d \geq 3$, and let $L/\mathbb{Q}$ be a degree d number field with Galois group S_d. Let N be the norm form of $L/\mathbb{Q}$. Then the (singular) $\mathbb{F}$-hypersurface*

$$X : N(X_1, \ldots, X_d) = tZ^d \tag{5}$$

has no $\mathbb{F}^{\mathrm{ab}}$-rational points.

Proof: Since $L/\mathbb{Q}$ is anabelian, it is linearly disjoint from $\mathbb{Q}^{\mathrm{ab}}$ and thus also from $\mathbb{K} = \mathbb{Q}^{\mathrm{ab}}((t^{\frac{1}{2}}))$. So the norm form of $L/\mathbb{Q}$ remains anisotropic over $\mathbb{K}$, and thus there are no $\mathbb{K}$-rational points on the hypersurface (5) with $Z = 0$. A solution with $Z \neq 0$ exists if and only if t is a norm from $\mathbb{M} = L \otimes_{\mathbb{Q}} \mathbb{K}$ to $\mathbb{K}$. But $\mathbb{M}/\mathbb{K}$ is an unramified extension of complete discretely valued fields, so the image of the norm map consists of elements whose valuation is divisible by d, whereas $v_{\mathbb{M}}(t) = v_{\mathbb{K}}(t) = 2$.

Corollary 22. *There is a geometrically rational surface $S_{/\mathbb{F}}$ without abelian points.*

Proof: Taking $d = 3$, one gets a geometrically integral cubic suface $S_{/\mathbb{F}}$ without abelian points, but with finitely many (in fact 3) singular points. We can resolve the singularities by a birational $\mathbb{F}$-morphism $\tilde{S} \rightarrow S$, and $S(\mathbb{F}^{\mathrm{ab}}) = \emptyset \implies \tilde{S}(\mathbb{F}^{\mathrm{ab}}) = \emptyset$.

Corollary 23. *For $d \geq 3$, there is a plane $\mathbb{F}$-curve of degree d without $\mathbb{F}^{\mathrm{ab}}$-points.*

Proof: The idea is as follows: since the singular locus of the hypersurface X of (5) is $(d-3)$-dimensional, intersecting with a general 2-plane gives a nonsingular curve.

Here are the details: let S be the singular locus of X. Since S has codimension 3 (and not 2!) in $\mathbb{P}^d$, there exists a nonempty open subset U_0 of the Grassmannian of

2-planes in $\mathbb{P}^d$ such that $p \in U_0$ implies $p \cap \operatorname{sing}(X) = \emptyset$. Now write S as a scheme-theoretic intersection of hypersurfaces $H_1, \ldots, H_n$. For each $1 \leq i \leq n$, we apply an affine Bertini theorem [8, Thm. 6.3] to $\mathbb{P}^d \setminus H_i$, obtaining a nonempty subset U_i of the aforementioned Grassmannian such that $p_i \in U_i$ implies $X \cap p_i$ is geometrically integral and has singular locus contained in H_i. It follows that for any $p \in \cap_{i=0}^n U_i$ (which is nonempty by the irreducibility of Grassmannians), $p \cap X$ is a nonsingular plane curve of degree d.

Taking $d = 4$ we get a genus 3 curve $C_{/\mathbb{F}}$ with $C(\mathbb{F}^{\text{ab}}) = \emptyset$.

Following [17], we get another approach to curves of genus 3 without abelian points:

Proposition 24. *Let F be a complete, discretely valued field whose residue field f contains an extension m which is Galois with group isomorphic to S_4. Then there exists a genus 3 curve $C_{/F}$ with $C(F^{\text{ab}}) = \emptyset$.*

Proof: After choosing an isomorphism of $G = \operatorname{Gal}(m/f)$ with S_4, we get an action of $\mathfrak{g}_f$ on the complete graph K_4 on 4 vertices. By [17, Prop. 4.6], there exists a stable curve $C_{/f}$ with rational geometric components, whose corresponding dual graph is isomorphic, as a $\mathfrak{g}_f$-module, to K_4 with the chosen G-action. By [17, Cor. 4.4], there exists a stable curve over the valuation ring R_F of F whose generic fiber is an honest (i.e., nonsingular and geometrically integral) curve $C_{/F}$ and whose special fiber is isomorphic to $C_{/f}$. Since the stabilizer of any vertex or edge of K_4 is a non-normal subgroup of S_4, after making any abelian residue extension f'/f, there are no $\mathfrak{g}_{f'}$-fixed vertices or edges of the dual graph, so $C(f') = \emptyset$. Hence if F'/F is any extension with abelian residue extension – so in particular if F'/F is itself abelian – $C(f') = \emptyset$ implies $C(R_{F'}) = C(F') = \emptyset$.

References

[1] S. Y. An, S. Y. Kim, D. C. Marshall, S. H. Marshall, W. G. McCallum, and A. R. Perlis, *Jacobians of genus one curves*, J. Number Theory **90** (2001), 304-315.

[2] P. L. Clark, *There are genus one curves of every index over every number field*, J. Reine Angew. Math. **594** (2006), 201–206.

[3] ———, *Period-index problems in WC-groups II: abelian varieties*, submitted.

[4] ———, *On the indices of curves over local fields*, to appear in *Manuscripta Math.*.

[5] M. Fried and M. Jarden, *Field Arithmetic*, Ergebnisse der Mathematik (3) **11** (1986).

[6] G. Frey, *Pseudo algebraically closed fields with non-Archimedean real valuations*, J. Algebra, **26** (1973), 202-207.

[7] L. Gerritzen. *Periode und Index eines prinzipal-homogenen Raumes über gewissen abelschen Varietäten*, Manuscripta Math. **8** (1973), 131-142.

[8] J. P. Jouanolou, *Théorèmes de Bertini et applications*, Progress in Math. **42** (1983).

[9] D. Kanevsky, *Application of the conjecture on the Manin obstruction to various Diophantine problems*, Astérisque, (1987), no. 147-148, 307-314, 345.

[10] S. Lang, *On quasi-algebraic closure*, Ann. of Math. **55** (1952), 373-390.

[11] S. Lang and J. Tate, *Principal homogeneous spaces over abelian varieties*, Amer. J. Math. **80** (1958), 659-684.

[12] S. Lichtenbaum, *The period-index problem for elliptic curves*, Amer. J. Math. **90** (1968), 1209-1223.

[13] B. Mazur, *On the passage from local to global in number theory*, Bull. Amer. Math. Soc. (N.S.) **29** (1993), 14-50.

[14] A. S. Merkurjev and A. A. Suslin. *K-cohomology of Severi-Brauer varieties and the normresidue homomorphism*, Math. USSR-Izv. 21 (1983), 307-340.
[15] J. Milne. *Arithmetic Duality Theorems*, Perspectives in Mathematics, 1. Academic Press Inc., 1986.
[16] K. Ono and C. Skinner, *Non-vanishing of quadratic twists of modular L-functions*, Invent. Math. **134** (1998), 651-660.
[17] A. Pál, *Solvable points on projective algebraic curves*, Canad. J. Math. **56** (2004), 612-637.
[18] J. P. Serre, *Corps locaux*, Hermann, Paris, 1962.
[19] ———, *Galois Cohomology*, Lecture Notes in Mathematics 5, 5th revised edition, Springer-Verlag, 1994.
[20] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics 106, Springer-Verlag, 1986.
[21] J. Tate, *WC-groups over p-adic fields*, Sem. Bourbaki, Exp. 156, 1957.
[22] W. C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. Ècole Norm. Sup. **2** (1969), 521-560.

The Mathematical Sciences Research Institute, 17 Gauss Way, Berkeley, CA 94709

Department of Mathematics, Boyd Graduate Studies Research Center, University of Georgia, Athens, GA 30602-7403, USA
E-mail address: pete@math.uga.edu