# CURVES OVER GLOBAL FIELDS VIOLATING THE HASSE PRINCIPLE

PETE L. CLARK

Abstract. We exhibit for each global field $k$ an algebraic curve over $k$ which violates the Hasse Principle. We can find such examples among Atkin-Lehner twists of certain elliptic modular curves and Drinfeld modular curves. Our main tool is a refinement of the "Twist Anti-Hasse Principle" (TAHP). We then use TAHP to construct further Hasse Principle violations, e.g. among curves over any number field of any given genus $g \geq 2$.

Contents



The author is partially supported by National Science Foundation grant DMS-0701771.

## Notation

For any field $k$, we write $\overline{k}$ for an algebraic closure of $k$ and $k^{\text{sep}}$ for a separable algebraic closure of $k$.

Let $k_0$ denote either $\mathbb{Q}$ or the rational function field $\mathbb{F}_p(t)$ for a prime number $p$. By a **global field** we mean a finite separable extension $k$ of $k_0$.

If $v$ is a place of $k$, we denote the completion by $k_v$. If $v$ is non-Archimedean, we denote by $R_v$ the ring of integers of $k_v$, $\mathfrak{m}_v$ the maximal ideal of $R_v$ and $\mathbb{F}_v = R_v/\mathfrak{m}_v$ the residue field. Let $\bar{\Sigma}_k$ denote the set of all places of $k$ and $\Sigma_k$ the set of all non-Archimedean places of $k$. We write $\mathbb{A}_k$ for the adèle ring over $k$.

A nice variety $V_{/k}$ is an algebraic $k$-variety which is smooth, projective and geometrically integral. A nice curve $C_{/k}$ is a nice algebraic variety of dimension one.

The characteristic exponent of a field $k$ is 1 if $\text{char}(k) = 0$ and otherwise is $\text{char}(k)$.

## 1. Introduction

### 1.1. Statements of results.

In this paper we systematically construct curves $C$ defined over any global field which have points everywhere locally – $C(\mathbb{A}_k) \neq \varnothing$ – but not globally: $C(k) = \varnothing$. In the language that we shall use in the sequel, we construct curves $C_{/k}$ which **violate the Hasse Principle** (or, for short, **violate HP**).

Curves violating HP have been of interest for almost 70 years, but most such constructions have been rather *ad hoc*. Our approach is more systematic and gives rise to HP violations over *any* global field which are both algorithmically effective and "natural" in that they involve curves of prior arithmetic geometric interest.

In order to state Main Theorem 1 we need to introduce some further notation.

Let $p$ be either 1 or a prime number. Let $k$ be a global field of characteristic exponent $p$, and let $M, N$ be odd prime numbers such that $M \geq 4$ and $M, N, p$ are pairwise coprime. The moduli problem which associates to a $\mathbb{Z}[\frac{1}{MN}]$-scheme $S$ the set of isomorphism classes of triples $(E, C, P)$, where $E_{/S}$ is an elliptic curve, $C \subset_S E[N]$ is a locally cyclic subgroup scheme of order $N$ and $P$ is an $S$-rational point of order $M$ is representable by a smooth, projective relative curve $X(N, M)_{/\mathbb{Z}[\frac{1}{MN}]}$. In particular, the modular curve $X(N, M)$ has a $k$-rational model.

**Main Theorem 1.** *Let $k/k_0$ be a global field of characteristic exponent $p$ and degree $d = [k : k_0]$. Then there exists an effectively computable constant $B = B(p, d)$ such that: for any odd prime numbers $M$, $N > B$ with $N \equiv -1 \pmod{M}$, there exists an infinite, effectively computable set $\{l_i\}$ of separable quadratic extensions of $k_0$ such that for all $i$, the twist $\mathcal{T}_i$ of $X(N, M)$ by the Atkin-Lehner involution $w_N$ and $l_i/k_0$ has points everywhere locally over $k_0$ and no $k$-rational points. It follows that for all $i$, the base extension $\mathcal{T}_i \otimes_{k_0} k$ of $\mathcal{T}_i$ to $k$ violates the Hasse Principle over $k$.*

When $\mathrm{char}(k) > 2$ we also construct Atkin-Lehner twisted Drinfeld modular curves which violate the Hasse Principle over $k$: Theorem 6.

**Main Theorem 2.** *Let $k$ be a global field, and let $g \geq 2$, $g' \geq 4$ be integers.*
*a) If $\mathrm{char}(k) = 0$, there exists a genus $g$ bielliptic curve $C_{/k}$ violating HP.*
*b) For any "non-elliptophilic" function field $k$ of odd characteristic, there exists a genus $g$ bielliptic curve $C_{/k}$ of genus $g$ violating HP.*
*c) If $k = \mathbb{F}(X)$ is a function field of odd characteristic, there exists a constant $d$ depending only on the genus of $X$ such that after making a degree $d$ constant extension $k \mapsto k\mathbb{F}_{q^d}$, there exists a genus $g$ bielliptic curve $C_{/k\mathbb{F}_{q^d}}$ violating HP.*
*d) If $\mathrm{char}(k)$ is odd, there is a genus $g'$ curve $C_{/k}$ violating HP.*

"Elliptophilic" is a neologism which is defined and studied in §4.3. A field can only be elliptophilic if its genus is large compared to the size of its constant subfield. We will show in particular that a function field of genus at most four is not elliptophilic.

Our main technique is a variant of the **Twist Anti-Hasse Principle** (TAHP) of [Cl08]. The version of TAHP presented in *loc. cit.* applies to curves over $\mathbb{Q}$. In §2 we prove a version of TAHP which is different in three respects. First, we work in the context of global fields of arbitrary characteristic. Second, we give additional conditions which suffice for the HP violation to persist over certain extensions of the ground field. Third, we no longer emphasize "prime twists" in the statements, although such considerations continue to play a role in the proofs in the form of using quadratic extensions which are ramified at as few finite places as possible.

The TAHP is proved in §2, and in §3 it is applied, together with results of Merel and Poonen, to prove Main Theorem 1. In §4 we prove Main Theorem 2.

The construction of genus one curves violating HP is outside of the scope of TAHP. In §5 we discuss how genus one counterexamples to HP can be related to the structure of Shafarevich-Tate groups of elliptic curves over the prime global subfield $k_0$. In §6 we explain how it is much easier to construct higher-dimensional varieties $V$ over any global field $k$ violating HP and discuss the prospect of passing from a variety violating HP to a subvariety which still violates HP.

### 1.2. **Provenance and acknowledgements.**

In February of 2009 B. Poonen wrote to the author:

"[D]o you know if this is a known result? There is an algorithm that takes as input a number field k, and produces a curve over k that violates the Hasse principle. (I just observed yesterday that this can be proved.)"

The author replied that he did not know a proof off-hand but was interested in the result and thought that it might be possible to prove it using Atkin-Lehner twists of modular curves. He was motivated to write the present paper upon seeing an early draft of Poonen's preprint [Po09]. The constructions of the present paper are independent of those of [Po09]. Nevertheless the impetus to consider the function field case came from Poonen's work.

Acknowledgements: I have been fortunate to receive a tremendous amount of feedback and help from many people over the relatively short time in which this paper was written. Thanks to D. Abramovich, J.-L. Colliot-Thélène, J.S. Ellenberg, E. Izadi, D.J. Lorenzini, D. Swinarski and (most of all) B. Poonen.

## 2. The Twist Anti-Hasse Principle Revisited

### 2.1. The Twist Anti-Hasse Principle.

**Theorem 1.** *(Twist Anti-Hasse Principle) Let $C_{/k}$ a nice curve and $\iota : C \to C$ a $k$-rational automorphism of order 2. Let $C/\iota$ be the quotient of $C$ by the group $\langle \iota \rangle$, so that there is a natural map $\Psi : C \to C/\iota$ of degree 2 and inducing a separable quadratic extension of function fields. Suppose:*
*(i) $\{P \in C(k) \mid \iota(P) = P\} = \varnothing$.*
*(ii) $\{P \in C(k^{\mathrm{sep}}) \mid \iota(P) = P\} \neq \varnothing$.*
*(iii) $C(\mathbb{A}_k) \neq \varnothing$.*
*(iv) $\#(C/\iota)(k) < \infty$.*
*Then there exist infinitely many separable quadratic extensions $l/k$ such that the twisted curve $\mathcal{T}(C, \iota, l/k)$ violates the Hasse Principle over $k$. We may take each $l/k$ to be the base change of a separable quadratic extension of the subfield $k_0$.*

*Proof.* Let $l/k$ be a separable quadratic extension. Then by $\mathcal{T}_l(C) := \mathcal{T}(C, \iota, l/k)$ we mean the $k$-variety obtained from the $l$-variety $C_{/l}$ by twisting the given $k$-structure by the cohomology class corresponding to $l$ in

$$H^1(k, \langle \iota \rangle) \cong H^1(k, \mathbb{Z}/2\mathbb{Z}) = \mathrm{Hom}(\mathrm{Gal}(k^{\mathrm{sep}}/k), \mathbb{Z}/2\mathbb{Z}).$$

More concretely, letting $\sigma_l$ denote the nonidentity element of $\mathrm{Gal}(l/k)$, the twisted $\mathrm{Gal}(l/k)$-action on $C(l)$ is given by $P \mapsto \iota(\sigma_l P)$. For each such $l$, we have natural set maps

$$\alpha_l : \mathcal{T}_l(C)(k) \hookrightarrow C(l),$$
$$\Psi_l : C(l) \to (C/\iota)(l).$$

Put

$$S_l = (\Psi_l \circ \alpha_l)(C_l(k)).$$

Then $S_l \subset (C/\iota)(k)$. Moreover, $(C/\iota)(k) = \bigcup_l S_l \cup \Psi(C(k))$, and for $l \neq l'$, $P \in S_l \cap S_{l'}$ implies that $P \in C(l) \cap C(l') = C(k)$. But $S_l \cap C(k)$ consists of $k$-rational $\iota$-fixed points, which we have assumed in (i) do not exist, so that for $l \neq l'$, $S_l \cap S_{l'} = \emptyset$. By (iv), $(C/\iota)(k)$ is finite, and we conclude that the set of $l$ for which $S_l \neq \emptyset$ is finite.

It therefore suffices to find infinitely many separable quadratic extensions $l$ such that $\mathcal{T}_l(C)$ has points everywhere locally.

We now consider cases, depending upon whether the characteristic of $k$ is zero, positive and odd, or equal to 2.

Case 1: $k$ has characteristic 0 (i.e., $k$ is a number field). Then Kummer theory applies to all quadratic extensions: every quadratic extension $l/k$ is separable and of the form $l = k(\sqrt{d})$ for some $d \in k \setminus k^{\times 2}$. Moreover $k(\sqrt{d}) = k(\sqrt{d'})$ iff $d \equiv d' \pmod{k^{\times 2}}$. Let us in fact take $l = k(\sqrt{d})$ with $d \in \mathbb{Q}$ of $k$. It will be notationally

convenient to think of the choice of $d$ – and hence $l = k(\sqrt{d})$ – as fixed: we may then abbreviate

$$\mathcal{T}C := \mathcal{T}_{k(\sqrt{d})}C.$$

To be sure, our main task is to demonstrate that there are infinitely many classes $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ such that $\mathcal{T}C$ has points everywhere locally.

First we require $d > 0$. This ensures that for every real place $v$ of $k$ (if any) we have $\mathcal{T}_l(C)(k_v) = C(k_v) \neq \varnothing$. Henceforth we need only worry about the finite places.

Let $R_d$ be the set of finite places that ramify in $l = k(\sqrt{d})$. Let $M_1$ be a positive integer such that for all places $v$ with $\#\mathbb{F}_v > M_1$, $C$ extends to a smooth relative curve $C_{/R_v}$ and such that every smooth curve of genus $g(C)$ over a finite field $\mathbb{F}$ with at least $M_1$ elements has an $\mathbb{F}$-rational point. We call a finite place $v$ **large** if $\#\mathbb{F}_v > M_1$ and $v \notin R_d$; otherwise $v$ is **small**. Note that for any fixed $d$, all but finitely many places are large.

We claim that for any large place $v$, $\mathcal{T}C(k_v) \neq \varnothing$. To see this, consider the minimal regular $R_v$-model for $\mathcal{T}C$. Since $v$ is large and $\mathcal{T}C$ becomes isomorphic to $C$ after the base change $k \mapsto k(\sqrt{d})$, the minimal regular $R_v$-model for $\mathcal{T}C$ becomes smooth after an unramified base change. However, smoothness is a geometric property and formation of the regular model commutes with unramified base change, so it must be the case that $\mathcal{T}C$ itself extends smoothly to $R_v$. Moreover, by assumption on $v$, there is an $\mathbb{F}_v$-rational point on the special fiber, so by Hensel's Lemma $\mathcal{T}C(k_v) \neq \varnothing$.

Now let $P$ be an $\iota$-fixed point, and put $K = k(P)$. Suppose that we can choose $d$ such that all small places $v$ split completely in $K$. Then since $\mathcal{T}C$ has $K$-rational points, it has $k_v$-rational points for all small places $v$, and hence it has points everywhere locally.

So it is enough to show the following: there exist infinitely many $d \in \mathbb{Q}^\times/Q^{\times 2}$ such that: $d > 0$, $k(d)/k$ is a quadratic extension, and for each finite place $v$ of $k$ such that either (i) $\#\mathbb{F}_v \leq M_1$ or (ii) $v$ ramifies in $k(d)/k$, we have that $v$ splits completely in $k(P)/k$. Let $\zeta_4$ be a primitive 4th root of unity. By Cebotarev density, the set $\mathcal{P}$ of primes of $\mathbb{Q}$ which split completely in the finite separable extension $k(P, \zeta_4)/\mathbb{Q}$ has positive density. More concretely, under the usual identification of finite places of $k_0$ with prime numbers, any element of $\mathcal{P}$ is a prime number $p \equiv 1 \pmod 4$, so that $k(\sqrt{p})/k$ ramifies only at primes of $k$ lying over $p$. Thus taking $d$ to be any element of $\mathcal{P}$, we get that $\mathcal{T}C$ has points everywhere locally.

Case 2: $k$ is a function field of odd characteristic $p$. Much of Case 1 still applies: in particular, quadratic extensions are governed by Kummer theory. The main difference is that the prime subfield is now $\mathbb{F}_p(t)$, so that its places correspond to irreducible polynomials $p_i(t) \in \mathbb{F}_p[t]$, together with the place corresponding to the point at infinity on the projective line. Arguing as above, it suffices to find infinitely many squarefree polynomials $d(t) \in \mathbb{F}_p[t]$ such that the corresponding quadratic extension $l = \mathbb{F}_p(t)(\sqrt{d(t)})/\mathbb{F}_p(t))$ ramifies only at places of $k_0$ which split completely

in $k(P)$. But the ramified places of $l/k$ correspond to the irreducible factors of $d(t)$, together with the place at infinity if and only if $d(t)$ has odd degree. By Cebotarev Density, there are infinitely many irreducible polynomials $p_i(t) \in \mathbb{F}_p[t]$ which split completely in $k(P)/k_0$. So taking $d = p_i(t)$ works provided $p_i(t)$ has even degree. Thus, if infinitely many $p_i$'s have even degree, we're done. Otherwise, by passing to a subseqence we may assume that all the $p_i$'s have even degree and take $d = f_i f_j$ for $i \neq j$.

Case 3: Suppose that $k$ has characteristic 2. Again most aspects of the proof go through, but in place of Kummer theory we must use Artin-Schreier theory, which turns out to be simpler. By Cebotarev, there exist infinitely many irreducible polynomials $p_i(t) \in \mathbb{F}_2[t]$ which split completely in the separable extension $k(P)/\mathbb{F}_2(t)$. The quadratic extension $l/k$ defined by the polynomial $X^2 + X = \frac{1}{p_i(t)}$ is then unramified at every place $v$ such that $v_p(\frac{1}{p_i(t)}) \geq 0$, i.e., at every place except the place corresponding to $p_i$. This completes the proof. □

### 2.2. **A corollary on base extension.**

**Corollary 2.** *Let $k/k_0$ be a global field. Suppose that we have a curve $C_{/k}$ and a $k$-rational involution $\iota$ satisfying hypotheses (i) through (iv) of Theorem 1. Suppose further that $K/k$ is a finite separable field extension such that the following hypotheses all hold:*
*$(i)_K$: There are no $K$-rational $\iota$-fixed points;*
*$(iv)_K$: $\#(C/\iota)(K) < \infty$.*
*Then there are infinitely many separable quadratic extensions $l/k_0$ such that the twisted curve $\mathcal{T}(C, \iota, lk/k) \otimes_k K$ violates the Hasse Principle over $k$.*

*Proof.* Observe that hypotheses (ii) and (iii) are stable under base change: since they hold over $k$, *a fortiori* they also hold over $K$. We may therefore apply Theorem 1 to the pair $(C, \iota)_{/K}$. For all but finitely many $l$'s, $Kl/K$ is a separable quadratic extension, and for such $l$ we have

$$\mathcal{T}(C_{/K}, \iota_{/K}, Kl/K) = \mathcal{T}(C, \iota, lk/k) \otimes_k K.$$

□

### 2.3. **Remarks on the satisfaction of the hypotheses.**

Recall [Cl08, Remark 1.2]: if a pair $(C, \iota)_{/k}$ satisfies the hypotheses of Theorem 1 then the genus of $C$ is at least 2 and the genus $g(C/\iota)$ of $C/\iota$ is at least one.

Let us consider some cases:

• $C/\iota$ has genus one and $0 < \#(C/\iota)(k) < \infty$. Then $C/k = E$ is an elliptic curve with finitely many $k$-rational points. Under these circumstances we can construct many pairs $(C, \iota)_{/k}$ satisfying the hypotheses of Theorem 1 and such that $C/\iota \cong E$: see Theorem 8 below. However, I do not know how to systematically produce extensions $K/k$ such that the hypotheses of Corollary 1 are satisfied: this is the notorious problem of growth of the Mordell-Weil group under field extension.

• $C/\iota$ has genus one and is a locally trivial but globally nontrivial torsor under

its Jacobian elliptic curve $E$. In this case $C/\iota$ itself already violates the HP over $k$. Moreover, upon base-changing to any finite extension $K/k$ which is not divisible by the index of $C/\iota$, we retain a HP violation.

• $k$ is a number field and $C/\iota$ has genus at least 2. In this case, Faltings' theorem asserts that $\#C(K) < \infty$ for every finite extension $K/k$, i.e., hypothesis $(\text{iv})_K$ of Corollary 2 holds for all extensions $K/k$. Therefore in order to apply Corollary 2 to $(C,\iota)_{/k}$ and $K/k$, we need only verify $(i)_K$: that $\iota$ has no $K$-rational fixed points. But this is a very mild hypothesis: if $C$ has no $k$-rational $\iota$-fixed points, then the set of $\overline{k}$-fixed points breaks up into a finite set of $\text{Gal}(\overline{k}/k)$-orbits, each of size greater than one. This means that there is a finite set of nontrivial Galois extensions $m_1,\dots,m_d/k$ such that for any finite extension $K/k$, $(\text{i})_K$ holds iff for all $i$, $K \not\supset m_i$.

Suppose now that instead of a single pair $(C,\iota)_{/k}$ we have an infinite sequence $(C_n,\iota_n)_{/k}$ of such pairs, then we get an infinite sequence of finite sets of nontrivial Galois extensions: $(\{m_{n,1},\dots,m_{n,d_n)}\})_{n=1}^{\infty}$. Make the following additional hypothesis (H): for every finite extension $K/k$, there exists $n \in \mathbb{Z}^+$ such that $K \not\supset m_{n,i}$ for all $1 \le i \le d_n$. Then $(\text{i})_K$, (ii), (iii), (iv) hold for $(C_n,\iota_n)$ and $K/k$, so that we get infinitely many HP violations $\mathcal{T}(C_n,\iota_n,Kl/K)$ over $K$.

• $k$ is a function field, $g(C/\iota) \ge 2$, and $C/\iota$ has transcendental moduli ("non-isotrivial"). By a theorem of P. Samuel [Sa, Thm. 4], for any finite field extension $K/k$, we have $\#(C/\iota)(K) < \infty$, and the discussion is the same as above.

• $k$ is a function field, $g(C/\iota) \ge 2$, and $C/\iota$ has algebraic moduli ("isotrivial"): $(C/\iota)_{/\overline{k}}$ has a model over some finite field $\mathbb{F}_q$. The set $(C/\iota)(k)$ need not be finite. Indeed, after enlarging the base so that $C/\iota$ is defined over a finite subfield $\mathbb{F}_q$ of $k$, as soon as there exists a single point $P \in (C/\iota)(k) \setminus (C/\iota)(\mathbb{F}_q)$, the orbit of $P$ under the $q$-power Frobenius map furnishes an infinite set of $k$-rational points.

Within the isotrivial case, a favorable subcase is that of constant curves: Let $k$ be a global field, and let $\mathbb{F}$ be the algebraic closure of $\mathbb{F}_p$ in $k$. We say that a curve $C_{/k}$ is **constant** if it has an $\mathbb{F}$-rational model. On the other hand, $k$ is itself the field of rational functions $\mathbb{F}(X)$ on a nice curve $X_{/\mathbb{F}}$, so that

$$C(k) = C(\mathbb{F}(X)) = \text{Hom}_{\mathbb{F}}(\text{Spec}\,\mathbb{F}(X), C_{/\mathbb{F}}),$$

and to every element $P$ of $C(k)$ is associated a point $P_C$ on the $\mathbb{F}$-scheme $C$. The point $P_C$ is closed iff $P \in C(\mathbb{F})$. Otherwise $P_C = \text{Spec}\,\mathbb{F}(C)$ is the generic point and $P$ corresponds to a finite morphism of $\mathbb{F}$-curves $\pi : X \to C$. If $C$ has positive genus, intuition suggests that the existence of such a morphism is "unlikely." More precisely, various hypotheses on $C$ and/or $X$ will rule out the existence of such a morphism, the simplest being $g(C) > g(X)$.

## 3. HP-violations from Atkin-Lehner twists of modular curves

### 3.1. **Number field case.**

We begin with the following setup, taken from [Cl08]. Let $N \in \mathbb{Z}^+$ be square-free, let $X_0(N)_{/\mathbb{Q}}$ denote the modular curve with $\Gamma_0(N)$-level structure, and let

$w_N$ denote the Atkin-Lehner involution, a $\mathbb{Q}$-rational involutory automorphism of $X_0(N)$. Let $k/\mathbb{Q}$ be a number field. We claim there exists an effectively computable $N_0$ such that for all squarefree $N > N_0$, $(X_0(N), w_N)$ satisfies hypotheses $(\text{i})_k$, (ii), (iii), $(\text{iv})_k$ of Corollary 2, and therefore there are infinitely many quadratic twists of $X_0(N)$ which violate the Hasse Principle over $\mathbb{Q}$ and also over $k$.

To see this, recall the following information from [Cl08] and the references cited therein: there are always geometric $w_N$-fixed points – i.e., hypothesis (ii) holds – and the least degree $[\mathbb{Q}(P) : \mathbb{Q}]$ of a $w_N$-fixed point is equal to the class number of $\mathbb{Q}(\sqrt{-N})$. By a famous result of Heilbronn, the class number $h(\mathbb{Q}(\sqrt{-N}))$ tends to infinity with $N$, so that hypothesis $(\text{i})_k$ holds for each number field $k$ and all $N \geq N_0(k)$, as above. Further, the cusp at $\infty$ is a $\mathbb{Q}$-rational point on $X_0(N)$, so (iii) holds. Moreover, the genus of $X_0^+(N) := X_0(N)/w_N$ is at least 2 for all $N \geq 133$. Therefore for $N \geq \max(N_0(k), 133)$, there are infinitely many quadratic extensions $l/k$ such that $\mathcal{T}(X_0(N), w_N, kl/k)$ violates the Hasse Principle.

Work of Gross-Zagier on the effective solution of Gauss' class number problem allows us to write down an explicit, though quite large, value of $N_0(k)$. But it is not necessary to know $N_0(k)$ explicitly in order to make the construction effective: rather, for a given $k$, one can simply search for an $N \geq 133$ such that $h(\mathbb{Q}(\sqrt{-N})) > [k : \mathbb{Q}]$. (Or, by genus theory, this will be the case for any $N$ which is divisible by sufficiently many primes.)

On the other hand, in order to get an explicit choice of $l$ we would need to explicitly determine all points of $X_0(N)$ which are defined over a quadratic extension of the number field $k$. This lies beyond the current state of knowledge of rational points on $X_0(N)$. However, we have a much better understanding of rational points on the coverings $X_1(N)$:

**Theorem 3.** *(Merel* [Me]*) For each positive integer $d$, there exists an effectively computable integer $M(d)$ such that if $P \in X_1(M)$ is any noncuspidal point with $[\mathbb{Q}(P) : \mathbb{Q}] \leq d$, then $M \leq M(d)$.*

Now let $N$ and $M$ be coprime squarefree positive integers with $M \geq 4$, and let $X(N, M)_{/\mathbb{Q}}$ be the modular curve with $\Gamma_0(N) \cap \Gamma_1(M)$-level structure. As recalled in §1, $X(N, M)_{/\mathbb{Q}}$ is a fine moduli space for the moduli problem $(E, C, P)_{/S}$: here $S$ is a $\mathbb{Q}$-scheme, $E_{/S}$ is an elliptic curve, $C \subset_S E[N]$ is a cyclic order $N$-subgroup scheme, and $P \in E(S)$ is a point of order $M$. The involution $w_N$ is defined on moduli as follows:

$$w_N : (E, C, P) \mapsto (E/C, E[N]/C, \iota(P)),$$

where $E/C$ is the quotient elliptic curve and $\iota$ is the isogeny $E \to E/C$. The canonical map $X(N, M) \to X_0(N)$ can be viewed on moduli as the forgetful map $(E, C, P) \mapsto (E, C)$, and the action of $w_N$ on $X_0(N)$ is the evident compatible one: $(E, C) \mapsto (E/C, E[N]/C)$. It follows that the $w_N$-fixed points of $X(N, M)$ – if any – lie over the $w_N$-fixed points of $X_0(N)$. Therefore, so long as $N$ is chosen sufficiently large with respect to the number field $k$ as above, since $(\text{i})_k$ holds for $w_N$ on $X(N)$, *a fortiori* it holds for $w_N$ on $X(N, M)$. As for any modular curve corresponding to a congruence subgroup, the cusp at $\infty$ gives a rational point on $X(N, M)$, so (iii) holds. Similarly, since there is a natural map $X(N, M)/w_N \to X_0(N)/w_N$, the curve $X(N, M)/w_N$ has genus at least 2 for all $N \geq 133$ and therefore $(\text{iv})_{/k}$ holds. Indeed, because of Merel's theorem we can be more explicit.

But first we need to verify (ii): that $X(N,M)$ has any $w_N$-fixed points at all. For any squarefree $N > 2$, one set of $w_N$-fixed points on $X_0(N)$ corresponds to the set of distinct isomorphism classes of elliptic curves $E$ with $\mathbb{Z}[\sqrt{-N}]$-CM, and $C$ is the kernel of the endomorphism $\iota = [\sqrt{-N}]$. (If $N \equiv 1 \pmod 4$, this is the entire set of $w_N$-fixed points. Otherwise, there is another set corresponding to elliptic curves with CM by the maximal order of $\mathbb{Q}(\sqrt{-N})$.) In order to get fixed points on $X(N,M)$, we wish to find an $M$-torsion point on a $\mathbb{Z}[\sqrt{-N}]$-CM elliptic curve with $\iota(P) = P$. Observe that $\iota(P) = P$ implies $P = \iota^2(P) = -NP$, so this is only possible if $(N+1)P = 0$, i.e., if $N \equiv -1 \pmod M$. Conversely, if $N \equiv -1 \pmod M$, then the characteristic polynomial of $\iota$ acting on $E[M]$ is $t^2 + N = t^2 - 1 = (t+1)(t-1)$, so there is an eigenvalue of 1, i.e., an $\iota$-fixed point.

Now we put all the ingredients together. Let $k$ be a number field, and put $d = [k : \mathbb{Q}]$. Let $M$ be an odd prime number which is larger than Merel's bound $M(2d)$. By Dirichlet's theorem on primes in arithmetic progressions, there exist infinitely many prime numbers $N$ such that $N \equiv -1 \pmod M$; choose one with $h(\mathbb{Q}(\sqrt{-N})) > d$. Then the curve $X(N,M)_{/\mathbb{Q}}$ satisfies $(\mathrm{i})_k$, (ii), (iii), (iv) of Corollary 2. Then $X(N,M)$ has no nonscuspidal rational points in any quadratic extension of $k$, so that there is an infinite, effectively computable set of quadratic extensions $l/\mathbb{Q}$ such that $\mathcal{T}(X(N,M), w_N, kl/k)$ violates the Hasse Principle over $k$.

We can say a bit more about the quadratic fields $l/\mathbb{Q}$ which work in the above construction. $X(N,M)$ is a quotient of the modular curve $X(NM)_{/\mathbb{Q}(\zeta_{NM}}$ with full $NM$-level structure. The cusps form a single orbit under the automorphism group of $X(NM)$. Since the cusp at $\infty$ is $\mathbb{Q}$-rational, it follows that all of the cusps are rational over the cyclotomic field $\mathbb{Q}(\zeta_{NM})$. Since none of the cusps are $w_N$-fixed points, it follows that if $l$ is not contained in $k(\zeta_{NM})$ the cuspidal points will not be rational over $\mathcal{T}(X(N,M), w_N, kl/k)_{k(\zeta_{NM})}$: thus only an explicit finite set of quadratic fields $l/\mathbb{Q}$ must be excluded.

### 3.2. **Function field case.**

Suppose now that $N$ and $p$ are disinct prime numbers, $k_0 = \mathbb{F}_p(t)$ and $k/k_0$ is a finite separable field extension, say with constant subfield $\mathbb{F}$. We again consider the elliptic modular curve $X_0(N)_{/k}$ and the Atkin-Lehner involution $w_N$. In this case $X_0(N)$ and $w_N$ are both defined over $\mathbb{F}_p$, so that the $w_N$-fixed points are algebraic over $\mathbb{F}_p$ and therefore separable over $k$. It follows that the quotient $X_0^+(N) = X_0(N)/w_N$ is isotrivial, so Samuel's theorem does not apply. But our curves are not only isotrivial but constant, so we can get away with a more elementary argument: if we choose $N$ sufficiently large so that the genus of $X_0^+(N)$ exceeds the genus of the curve $X$ such that $k = \mathbb{F}(X)$, we must have $X_0(k) = X_0(\mathbb{F})$, which is certainly finite. As we will see shortly, by further choosing $N$ suitably in terms of $p$, the hypotheses of Theorem 1 do apply to $(X_0(N), w_N)_{/k}$, so that we get HP violations.

In order to make this result effective we would need an explicit description of the $\mathbb{F}$-rational points on $X_0^+(N)$. This can certainly be done, e.g., using the Eichler-Selberg trace formula. However, it seems cleaner (and, arguably, more interesting) to adapt the argument given in the number field case. We can still get HP violations

using the modular curves $X(N,M)$ as above provided that we have an analogue of Merel's theorem, i.e., a result which tells us that for fixed $[k:k_0]$ and sufficiently large $M$, the only $k$-rational points on $X_1(M)$ are the cusps. Such a result has indeed been proven, by B. Poonen. We first introduce some notation:

Let $K$ be a field of characteristic $p > 0$, and let $E_{/K}$ an elliptic curve with transcendental $j$-invariant. Thus $E$ is ordinary. Let

$$\rho_E : \mathrm{Gal}_K \to \mathbb{Z}_p^\times \times \prod_{\ell \neq p} GL_2(\mathbb{Z}_\ell) = \mathrm{Aut}(E(K^{\mathrm{sep}}[\mathrm{tors}]) = \mathrm{Aut}\left(\mathbb{Q}_p/\mathbb{Z}_p \oplus \bigoplus_{\ell \neq p} (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^2\right)$$

be the homomorphism attached to the $\mathrm{Gal}_K$-module $E(K^{\mathrm{sep}})[\mathrm{tors}]$. Put

$$S = \mathbb{Z}_p^\times \times \prod_{\ell \neq p} SL_2(\mathbb{Z}_\ell).$$

**Theorem 4.** *(Poonen,* [Po07]*) For every $d \in \mathbb{Z}^+$, there exists a constant $N(p,d)$ such that: for any field $k$ of characteristic $p > 0$, any field extension $K/k(t)$ of degree at most $d$, and any elliptic curve $E_{/K}$ with transcendental $j$-invariant, the index $[S : \rho_E(\mathrm{Gal}(K^{\mathrm{sep}}/K)) \cap S]$ is at most $N(p,d)$.*

From this we readily deduce the desired boundedness result.

**Corollary 5.** *Let $p$ be a prime number and $k_0 = \mathbb{F}_p(t)$. Then, for every positive integer $d$, there exists a constant $B(p,d)$ such that: for any finite field extension $K/k_0$ of degree at most $d$ and any prime number $M > \max(3, p, B(p,d))$, the only $K$-rational points on $X_1(M)$ are cusps.*

*Proof.* Let $K/k_0$ be an extension of degree $d' \leq d$, let $M > \max 3, p, N(p,d)$ be a prime number, and suppose that $X_1(N)$ has a noncuspidal $K$-rational point. Since $M \geq 4$, $Y_1(M)$ is a fine moduli space, and there is a corresponding pair $(E,P)_{/K}$, where $E$ is an elliptic curve and $P \in E(K)$ is a point of order $M$. There is then is a basis for $E[M](K^{\mathrm{sep}})$ with respect to which the mod $M$ Galois representation has image contained in the subgroup $T(M) \subset \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$ of matrices

$$\{\left[\begin{array}{cc} 1 & b \\ 0 & d \end{array}\right] \mid b \in \mathbb{Z}/M\mathbb{Z},\ d \in (\mathbb{Z}/M\mathbb{Z})^\times\}.$$

Since $\#T(M) \cap \mathrm{SL}_2(\mathbb{Z}/M\mathbb{Z}) = M$, the index of the full Galois representation is at least $\#SL_2(\mathbb{Z}/M\mathbb{Z})/M = M^2 - 1 > M$. Applying Theorem 4, we conclude that $j(E)$ must be algebraic. Let $\mathbb{F}$ be the algebraic closure of $\mathbb{F}_p$ in $K$. Because the order of the automorphism group of any elliptic curve divides 24, it follows that there is an extension $\mathbb{F}'/\mathbb{F}$ of degree dividing 24 and an elliptic curve $E'/\mathbb{F}'$ such that $E'_{/F'K} \cong E_{/\mathbb{F}'K}$. Moreover, since $E'$ is defined over $\mathbb{F}'$, all the torsion is defined over an algebraic extension of $\mathbb{F}'$, hence the torsion field $\mathbb{F}'(P)$ is linearly disjoint from $\mathbb{F}'K$ over $F$, so $[\mathbb{F}'(P) : \mathbb{F}''] = [\mathbb{F}'K(P) : \mathbb{F}'K] = 1$, i.e., $P$ is already $\mathbb{F}'$-rational. On the other hand, the degree of $\mathbb{F}'$ over $\mathbb{F}_p$ is at most $24[K : k_0] \leq 24d$, so that $\#\mathbb{F} \leq p^{24d}$ and hence (applying the Hasse bound)

$$M \leq \#E(\mathbb{F}') \leq (p^{12d} + 1)^2.$$

Thus it suffices to take

$$B(p,d) = \max\left(3, p, N(p,d), (p^{12d} + 1)^2\right).$$

□

We can now establish the function field case of Main Theorem 1 by an argument very similar to that used in the number field case, replacing our appeal to Merel's Theorem 3 with an appeal to Corollary 5.

Indeed, let $k/\mathbb{F}_p(t)$ be a finite separable extension; put $d = [k : \mathbb{F}_p(t)]$. Let $M$ be a prime number which is greater than the constant $B(p, 2d)$ of Corollary 5. By Dirichlet's theorem on primes in arithmetic progressions combined with the Chinese Remainder Theorem, there exist infinitely many prime numbers $N$ such that $N \equiv -1 \pmod{M}$ and $-N$ is a quadratic residue mod $p$. If $p = 2$ the last condition is vacuous, so we require moreover that $-N \equiv 1 \pmod{8}$. Thus $p$ splits in $\mathbb{Q}(\sqrt{-N})$. We claim that if $N$ is sufficiently large, $X_0(N)$ – and, *a fortiori*, $X(N, M)$ – has no $k$-rational $w_N$-fixed points. Let $d(N, p)$ be the least degree of a $w_N$-fixed point on $X_0(N)_{/\mathbb{F}_p}$. By the modular interpretation of Atkin-Lehner fixed points recalled above, we have

$$d(N, p) = [\mathbb{F}_p(j(E)) : \mathbb{F}_p],$$

where $E/_{\overline{\mathbb{F}_p}}$ is any elliptic curve with complex multiplication by the maximal order of $\mathbb{Q}(\sqrt{-N})$ and $j(E)$ is its $j$-invariant. Now we recall Deuring's correspondence: reduction modulo $p$ induces a bijection from the set of the $j$-invariants of $K$-CM elliptic curves in characteristic 0 for which $p$ splits in the CM field $K$ to the set of $j$-invariants of ordinary elliptic curves over $\overline{\mathbb{F}_p}$ [La87, Thm. 13.13]. Since there are, of course, only finitely many $j$-invariants lying in an extension of $\mathbb{F}_p$ of degree at most $d$, this shows that for fixed $p$ and $N$ lying in the above infinite set of primes, $d(N, p)$ approaches infinity with $N$. Thus for all sufficiently large $N$, $w_N$ has no $k$-rational fixed points: hypothesis $(i)_k$ holds. Moreover, our choice of $M$ implies that $X(N, M)/w_N$ has only cuspidal $k$-rational points, so hypothesis $(iv)_k$ holds. We have at least one $\mathbb{F}_p$-rational cusp, so hypothesis (iii) holds. Finally, hypothesis (ii) certainly holds: we can either use the same argument as we did in characteristic 0 or simply observe that it follows from the characteristic 0 case by specialization. Therefore Corollary 2 applies, completing the proof of Main Theorem 1 in the function field case.

### 3.3. **A Complement: Drinfeld modular curves.**

Let $k$ be a global function field of characteristic $p > 2$. As we saw, Samuel's theorem does not apply to the modular curves $X(N, M)_{/k}$. One may view this as a hint that we have chosen "the wrong modular curves" for the function-field version of the argument. Indeed, a family of curves with properties highly analogous to those of modular curves over number fields and to which Samuel's theorem does apply are the Drinfeld modular curves.

Specifically, take $A = \mathbb{F}_p[t]$ and for $\mathfrak{n}$ a nonzero prime ideal of $A$ (which we identify with the corresponding monic irreducible polynomial) there is a curve $X_0(\mathfrak{n})_{/k_0}$ and a canonical $k_0$-rational involutory automorphism $w_\mathfrak{n}$. The involution $w_\mathfrak{n}$ always has separable fixed points, and the least degree of a fixed point is equal to the class number $h(\mathfrak{n})$ of the "imaginary quadratic field" $k_0(\sqrt{\mathfrak{n}})$. Both $h(\mathfrak{n})$ and the genus

of $X_0(\mathfrak{n})/w_{\mathfrak{n}}$ tend to infinity with the norm of $\mathfrak{n}$. Moreover $X_0(\mathfrak{n})$ has at least one $k_0$-rational cusp. (For all these facts, see [Ge86], [Ge01].) Therefore:

**Theorem 6.** *For each fixed odd prime $p$ and finite separable extension $k/k_0$, there exists $N = N(p,k)$ such that for all primes $\mathfrak{n}$ of norm larger than $N$, there are infinitely many separable quadratic extensions $l/k_0$ such that the Atkin-Lehner twist of $X_0(\mathfrak{n})$ by $w_{\mathfrak{n}}$ and $kl/k$ violates the Hasse Principle.*

However, there are two differences from the classical modular case.

One the one hand, the analogue of Merel's theorem is not yet available: the uniform boundedness of torsion points on rank 2 Drinfeld modules is believed to be true but remains open. Thus, consideration of Drinfeld modular curves with $\Gamma_0(\mathfrak{n}) \cap \Gamma_1(\mathfrak{m})$-level structure would not help to make the constructive effective.

On the other hand, this help is not needed, because work of Szpiro [Sz] makes Samuel's theorem effective (c.f. [Po09, Lemma 2.1]).

We therefore have another way of answering Poonen's question for function fields of positive, odd characteristic.[1]

### 3.4. **Poonen's theorem.**

The main result of Poonen's paper [Po09, Thm. 1.1] is stronger than the one mentioned in the introduction. He proves:

**Theorem 7.** *(Poonen) There is an algorithm which takes as input a global field $k$ and $n \in \mathbb{N}$ and returns a nice algebraic curve $C_{/k}$ with $C(\mathbb{A}_k) \neq \varnothing$ and $\#C(k) = n$.*

The proof of Main Theorem 1 leads to a proof of Theorem 7 as well. This is done in much the same way as in [Po09], but we feel that the result is interesting enough to be included here as well as in *loc. cit.*

The idea is as follows: we have already proved Theorem 7 in the case $n = 0$. In the remaining case $n > 0$ – in which case $C(\mathbb{A}_k) \neq \varnothing$ is automatic – it suffices to find the following: for any global field $k$, a curve $C_{/k}$ in which the set $C(k)$ is nonempty, finite and effectively computable. Then by a simple weak approximation argument, we can build a finite, separable branched covering $\pi : C' \to C$ which has prescribed local behavior at each of the finitely many fibers containing a $k$-rational point. In particular, for each $P \in C(k)$, we may arrange for the fiber over $P$ to contain $n_P$ rational points, for any $0 \neq n_P \leq \deg(\pi)$. In particular, for any $n \geq 2$, by building a covering of degree $n$, requiring one of the $k$-rational points to split completely into $n$ rational points, and requiring the fibers to be irreducible over the remaining $k$-rational points, we get a curve $C'$ with exactly $n$ rational points. We proceed similarly for $n = 1$, except we need to use a covering of degree at least 2.

Starting from scratch, it is no trivial matter to produce such a curve $C$ over an arbitrary global field. Fortunately we have already done so: we observed above that for fixed $k$ and sufficiently large $N$, the only rational points on the curves $X(N,M)_{/k}$ are the cusps, which are finite in number, have effectively computable

[1] It seems likely that the argument works also in characteristic 2. Our restriction is due to the lack of a suitable reference on Atkin-Lehner fixed points on Drinfeld modular curves over $\mathbb{F}_2(t)$.

(indeed, well-known) fields of definition, and for which at least one is rational over $k_0$. This is enough to prove Theorem 7.

## 4. HP-violations with prescribed genus

### 4.1. **A criterion for bielliptic HP violations.**

**Theorem 8.** *Let $k$ be a global field of characteristic different from 2. We **suppose** that there exists an elliptic curve $E_{/k}$ with $E(k)$ finite. Then for each integer $g \geq 2$, there exists a bielliptic curve $C_{/k}$ of genus $g$ which violates HP.*

*Proof.* Let $E_{/k}$ be as in the statement of the theorem. Let $q : E \to \mathbb{P}^1$ be the degree 2 map obtained by quotienting out by the involution $[-1]$. (In more elementary terms, $q : (x, y) \mapsto x$.) By hypothesis, for all but finitely many points $x \in \mathbb{P}^1(K)$, the pullback of the degree one divisor $[x]$ on $\mathbb{P}^1$ is the degree 2 divisor $[P] + [-P]$ such that the field of definition of $P$ is a quadratic extension of $k$. Moreover, for every finite extension $l/k$, the set $q(E(l))$ of $x$-coordinates of $l$-rational points of $E$ is **thin** in the sense of [Se, §3.1]. Since $k$ is a Hilbertian field, it follows that we can choose $g-1$ points $x_i \in k(\mathbb{P}^1)$ such that the fields of definition of the points $[P_i]$, $[-P_i]$ in the pulled back divisor $D_i = [P_i] + [-P_i] = q^*([x_i])$ are distinct quadratic extensions $l_1, \ldots, l_{g-1}$ of $k$. In particular, the $D_i$'s have pairwise disjoint supports.

Next, note that all of the $D_i$'s are linearly equivalent to each other, and also to $q^{-1}([\infty]) = 2[O]$. Therefore the divisor

$$D := \sum_{i=1}^{g-1} D_i - (2g-2)[O]$$

is linearly equivalent to zero on $E$, so it is the divisor of a function $f \in k(E)$. Moreover, we have the leeway of multiplying $f$ by any nonzero element $a$ of $k$ without changing its divisor, and it is easy to see that by an appropriate choice of $a$, we can arrange for the pullback of the divisor $[O]$ in the twofold cover $C$ of $E$ defined by the equation $y^2 = \sqrt{af}$ to consist of two distinct, $k$-rational points. The curve $C$ is ramified at the $2(g-1)$ distinct points comprising the support of $D_i$, so by Riemann-Hurwitz has genus $(g-1)+1 = g$. We may view the twofold covering $C \to E$ as being the quotient by an involution $\iota$ on $C$, and one immediately verifies that the pair $(C, \iota)$ satisfies hypotheses (i) through (iv) of Theorem 1. □

Remark 4.1.1: In order to make Theorem 8 effective, we need to be able to find an elliptic curve $E_{/k}$ with $E(k)$ finite and effectively computable. We believe that in all our applications of this result this is actually possible, but not having checked the details we do not advertise it.

### 4.2. **Proof of Main Theorem 2a).**

We can now give the proof of Main Theorem 2a). The missing piece is the following recent, spectacular result of Mazur and Rubin: for every number field $k$, there exist infinitely many elliptic curves $E_{/k}$ with $E(k) = 0$ [MR, Cor. 1.9]. Therefore Theorem 8 applies to give the desired result.

Remark 4.2.1: Genus one counterexamples to HP over $\mathbb{Q}$ were first constructed by Lind and Reichardt. (See §5 for some further discussion of the genus one case.)

D. Coray and C. Manoil showed [CM, Prop. 4.2, 4.4] that for every $g \geq 2$ there exists a hyperelliptic curve $C_{/\mathbb{Q}}$ of genus $g$ violating HP. Using Wiles' theorem on rational points on Fermat curves, they also gave [CM, Prop. 4.5] examples of non-hyperelliptic HP violations of genus $4k^2$ for any $k \geq 1$.

Remark 4.2.2: Any nice curve of genus 2 is hyperelliptic. A nice nonhyperelliptic curve of genus 3 is (canonically embedded as) a plane quartic curve. Bremner, Lewis and Morton have shown [BLM] that the nice plane quartic

$$C_{/\mathbb{Q}} : 3X^4 + 4Y^4 = 19Z^4$$

violates HP. For $g \geq 4$ a bielliptic curve of genus $g$ is not hyperelliptic [ACGH, Exercise C-2, p. 366], so it follows from Main Theorem 2a) that nonhyperelliptic HP violations over $\mathbb{Q}$ exist in every conceivable genus.

### 4.3. **Elliptophilic curves.**

Let $k$ be a function field of characteristic $p$ and with field of constants $\mathbb{F}$. It seems likely that there is an elliptic curve $E_{/k}$ with $E(k)$ finite.[2] In this section we observe that by restricting attention to *constant* elliptic curves $E_{/\mathbb{F}}$, we can already prove this in many cases.

Namely, let $X_{/\mathbb{F}}$ be the nice curve corresponding to the function field $k$, and let $E_{/\mathbb{F}}$ be an elliptic curve, viewed by extension of scalars as a constant elliptic curve over $k$. Then $E(k) \supsetneq E(\mathbb{F})$ if and only if there exists a finite $\mathbb{F}$-morphism $X \to E$ iff $E_{/k}$ is one of the finitely many $\mathbb{F}$-isogeny factors of the Jacobian abelian variety $\mathrm{Jac}(X)$. Thus, for a fixed $k$, there does not exist any constant elliptic curve $E_{/k}$ with $E(k) = E(\mathbb{F})$ (hence finite) iff the Jacobian of $X$ contains as an isogeny factor every $\mathbb{F}$-isogeny class of elliptic curves.

This is a curious property for a curve $X_{/\mathbb{F}}$ to have. Let us study it further:

A nice curve $X$ over a finite field $\mathbb{F}$ is **elliptophilic** if for every elliptic curve $E_{/\mathbb{F}}$ there exists a finite $\mathbb{F}$-morphism $C \to E$. Equivalently, $X$ is elliptophilic if every $\mathbb{F}$-isogeny class of $\mathbb{F}$-rational elliptic curves appears as an isogeny factor of $\mathrm{Jac}(X)$. Now we make some observations:

• If $X_{/\mathbb{F}}$ is elliptophilic, and $Y \to X$ is a branched covering of $X$, then $Y$ is also elliptophilic. Thus if there is one elliptophilic curve $X_{/\mathbb{F}}$, there are infinitely many.

• For any finite field $\mathbb{F}$, there exists an elliptophilic curve $X_{/\mathbb{F}}$.

*Proof.* Let $A = \prod_{i=1}^N E_i$ be a product of elliptic curves containing each $E_{/\mathbb{F}}$ up to isogeny at least once. It follows from [Po04, Thm. 3.7] that there exists a nice curve $X \subset A$ such that the induced map on Albanese varieties $\mathrm{Jac}(X) \to A$ is surjective. Then $X_{/\mathbb{F}}$ is elliptophilic. □

[2]Indeed, conceivably the methods of [MR] could be carried over to this context, but exploration of this is beyond the scope of this paper.

• Let $\mathbb{F} = \mathbb{F}_q = \mathbb{F}_{p^a}$. If $X_{/\mathbb{F}_q}$ is elliptophilic, then its genus $g(X)$ satisfies

$$g(X) \geq \max\left(2\lfloor 2\sqrt{q}\rfloor(1-\frac{1}{p}), 5\right).$$

*Proof.* An elliptophilic curve $X_{/\mathbb{F}}$ must have genus at least as large as the number of $\mathbb{F}$-isogeny classes of elliptic curves. Since two elliptic curves over $\mathbb{F}$ are $\mathbb{F}$-isogenous iff they have the same number of $\mathbb{F}$-rational points, it comes down to the Deuring-Waterhouse theorem enumerating the possible orders of the finite groups $E(\mathbb{F})$ [Wa, Thm. 4.1]. We need not recall the full statement, but only the following parts:
(i) $|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$;
(ii) for any positive integer $t$ with $\gcd(t,p) = 1$ and $|q+1-t| \leq 2\sqrt{q}$, there exists an elliptic curve $E_{/\mathbb{F}_q}$ with $\#E(\mathbb{F}_q) = t$;
(iii) if $a = \log_p q$ is odd, there exists $E_{/\mathbb{F}_q}$ with $\#E(\mathbb{F}_q) = q+1$;
(iv) if $a$ is even, there exists $E$ (resp. $E'$) over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q+1+2\sqrt{q}$ (resp. $\#E'(\mathbb{F}_q) = q+1-2\sqrt{q}$).
It follows that there are at least $2\lfloor 2\sqrt{q}\rfloor(1-\frac{1}{p})$ isogeny classes. Moreover, $2\lfloor 2\sqrt{q}\rfloor(1-\frac{1}{p}) \geq 5$ if $p > 3$, if $q = 3^a$ with $a \geq 2$, or if $q = 2^a$ with $a \geq 3$, and one verifies that for $q = 2, 3, 4$ there are precisely 5, 7, and 9 rational isogeny classes of elliptic curves over $\mathbb{F}_q$, respectively. □

An easy computation now yields:

**Corollary 9.** *Let $k$ be the function field of a nice curve $X_{/\mathbb{F}_q}$. Let $d$ be the least even integer greater than $\log_q g(X) - 2\log_q(\frac{4p-4}{p})$. Then the curve $X_{/\mathbb{F}_{q^d}}$ is not elliptophilic: there exists an elliptic curve $E_{/\mathbb{F}_{q^d}}$ such that $E(k\mathbb{F}_{q^d}) = E(\mathbb{F}_{q^d})$.*

Remark 4.3.1: We do not know whether there exists a genus 5 elliptophilic curve $X_{/\mathbb{F}_2}$, nor in fact do we know any concrete examples of elliptophilic curves. To find some seems to be an interesting computational project.

### 4.4. **Proof of Main Theorem 2b), 2c).**

Combining Theorem 8 and Corollary 9 we immediately deduce the following, a more detailed version of parts b) and c) of Main Theorem 2.

**Theorem 10.** *Let $k = \mathbb{F}_q(X)$ be a function field of characteristic $p > 2$.*
*a) If $X_{/\mathbb{F}_q}$ is* not *elliptophilic, then for all $g \geq 2$, there exists a bielliptic curve $C_{/k}$ of genus $g$ violating HP.*
*b) The hypothesis of part a) holds if*

$$g(X) < \max\left(2\lfloor 2\sqrt{q}\rfloor(1-\frac{1}{p}), 5\right).$$

*c) Let $d$ be the least even integer greater than $2\log_q g(X) - 2\log_q(\frac{4p-4}{p})$. After making the degree $d$ constant extension $\mathbb{F}_q \mapsto \mathbb{F}_{q^d}$, for all $g \geq 2$, there exists a bielliptic curve $C_{/k\mathbb{F}_{q^d}}$ of genus $g$ violating HP.*

### 4.5. **Proof of Main Theorem 2d).**

Over any global field $k$ with $\mathrm{char}(k) \neq 2$, we get the following result, a slight sharpening of Main Theorem 2d).

**Theorem 11.** *Let $k$ be a global field of characteristic not equal to 2 and $g' \geq 4$ an integer. Then there are infinitely many curves $C_{/k_0}$ of genus $g'$ such that the base change of $C$ to $k$ violates HP.*

*Proof.* Fix $g_0 \geq 2$, and let $P(x) \in k[x]$ be a monic polynomial of degree $2g_0 + 1$ with distinct roots in $k^{\mathrm{sep}}$. When $\mathrm{char}(k_0) = p > 0$, we require that $P$ is not $PGL_2$-equivalent to a polynomial defined over $\overline{\mathbb{F}_p}$. Then

$$X : y^2 = P(x)$$

defines a nonisotrivial hyperelliptic curve of genus $g_0$ with a $k$-rational Weierstrass point $O$. Let $q : X \to \mathbb{P}^1$ denote the hyperelliptic involution. Exactly as in the previous construction, for any $d \geq 1$ we may choose $d$ points $x_i \in \mathbb{P}^1(k)$ such that $D_i := q^*([x_i]) = [P_i] + [q(P_i)]$, such that the residue fields $l_i$ of $P_i$ are distinct quadratic extensions of $k$. Now take

$$D = \sum_{i=1}^{d} D_i - 2d[O],$$

and choose $f \in k(X)$ with $\mathrm{div}(f) = D$ such that $O$ splits into 2 $k$-rational points on the corresponding 2-fold cover $C \to X$ defined by the extension $k(X)(\sqrt{f})/k(X)$. By Riemann-Hurwitz, the genus of $C$ is $g = 2g_0 + d - 1$. Writing $\iota$ for the induced involution on $C$, the pair $(C, \iota)$ satisfies all the hypotheses of Theorem 1, so that there are infinitely many twists which violate HP over $k$. Taking $g_0 = 2$, we get curves of every genus $g' \geq 4$.

Now if we require that $P$ has $k_0$-coefficients, then the construction can be carried out over $k_0$ by taking $k_0$-rational points on $\mathbb{P}^1$ and ensuring that at least one of the quadratic extensions $l_i/k_0$ is not contained in $k$ (this is why we showed in the proof of Theorem 8 that infinitely many quadratic extensions were possible). Then the hypotheses of Corollary 2 are satisfied, so that we get infinitely many curves of any given $g' \geq 4$ which are defined over $k_0$ and violate HP over $k$. □

## 5. Conjectures on HP violations in genus one

We wish to consider some conjectures involving HP violations on curves of genus one and the logical relations between them.

**Conjecture 1.**
*For every global field $k$, there is a genus one curve $C_{/k}$ which violates the Hasse Principle. Equivalently, there is an elliptic curve $E_{/k}$ with $Ш(k, E) \neq 0$.*

The most important conjecture on Shafarevich-Tate groups is, of course, that they are all finite. More precisely, say that a global field $k$ is Ш-**finite** if $Ш(k, E)$ is finite for all elliptic curves $E_{/k}$. It is expected that every global field is Ш-finite. The following observation is mostly for amusement:

**Proposition 12.** *Suppose that the prime global subfield $k_0$ is* not *Ш-finite. Then for every finite field extension $k/k_0$, there exists a genus one curve $C_{/k}$ violating the Hasse Principle.*

*Proof.* Our assumption is that there exists an elliptic curve $E_{/k_0}$ with $\#Ш(k_0, E) = \infty$. Since for all $n \in \mathbb{Z}^+$, $Ш(k_0, E)[n]$ is finite, the infinitude of $Ш(k_0, E)$ means that it contains elements of arbitarily large order. In particular, if $k/k_0$ is a field extension of degree $d$, then let $C$ be a genus one curve corresponding to a class

$\eta \in Ш(k_0, E)$ of order strictly greater than $d$. Then the index of $C$ is strictly greater than $d$, and since $C$ has genus one, this implies that the least degree of a closed point exceeds $d$, so that we must have $C(k) = \varnothing$. □

The proof of Proposition 12 also shows that Conjecture 1 is implied by the following

**Conjecture 2.** *For $n, k \in \mathbb{Z}^+$ with $n > 1$, there exists an elliptic curve $E_{/k_0}$ such that $Ш(k_0, E)$ has at least $k$ elements of order $n$.*

Conjecture 2 however seems to lie much deeper than Conjecture 1. When $k_0 = \mathbb{Q}$, Conjecture 2 is known to hold for $n = 2$ [Bo], $n = 3$ [Ca] $n = 5$ [Fis], $n = 7$ – [Ma07] and independently, S. Donnelly, unpublished – and $n = 13$ [Ma07]. The proofs all make heavy use of the fact that the modular curve $X_0(n)$ has genus zero for these values of $n$, and, conversely these are the only prime numbers $n$ such that $X_0(n)$ has genus 0. In [Ma06], Matsuno makes reference to as yet unpublished work of K. Naganuma claiming similar results over many quadratic extensions of $k_0$ when $X_0(n)$ has genus one. Decidedly new ideas seem to be needed to handle the remaining cases.

Remark 5.1: The author is not aware of any work on the $k_0 = \mathbb{F}_p(t)$ analogues of these results. Nevertheless one expects that similar results can be proven, at least as long as one avoids the case $p \mid n$.

The HP-violations constructed in §3 all had the property that they were base extensions of HP violations of the prime global subfield. It is natural to consider such constructions in genus one:

**Conjecture 3.** *For every global field $k$, there is a genus one curve $C$ defined over $k_0$ such that $C$ violates the Hasse Principle over $k_0$ and also over $k$.*

Evidently Conjecture 2 $\implies$ Conjecture 3 $\implies$ Conjecture 1. One pleasant aspect of Conjecture 3 is that it suffices to prove it for $k$ sufficiently large, e.g. Galois over $k_0$ and containing sufficiently many roots of unity for Kummer theory to apply.

## 6. Passage to a subvariety

### 6.1. Restriction of scalars and HP violations.

Let $k$ be a global field, $l/k$ a finite separable field extension, and $V_{/l}$ a nice variety. Recall that there is a $k$-variety $W = (\mathrm{Res}_{l/k} V)$, called the **Weil restriction** of $V$, whose functor of points on affine $k$-schemes is as follows: $\mathrm{Spec}\, A \mapsto V(A \otimes_k l)$. Taking $A = k$, we get

$$W(k) = V(k \otimes_k l) = V(l),$$

and taking $A = \mathbb{A}_k$, we get

$$W(\mathbb{A}_k) = V(\mathbb{A}_k \otimes l) = V(\mathbb{A}_l),$$

so that $V$ violates the Hasse Principle over $l$ iff $W = \mathrm{Res}_{l/k} V$ violates the Hasse Principle over $k$. Moreover, if $V$ is smooth, projective and geometrically integral, then $W$ is smooth, projective and geometrically integral, and of dimension $[l : k] \dim V$. That is to say, a Hasse Principle violation over any finite separable extension $l/k$ gives rise to a Hasse Principle violation over $k$, at the expense of multiplying the dimension by $[l : k]$.

6.2. **HP violations from torsors under abelian varieties.**

**Theorem 13.** *Let $k$ be any global field. Then there exists an abelian variety $A_{/k}$ and a torsor $W_{/k}$ under $A$ such that $W$ violates the Hasse Principle over $k$.*

*Proof.* Suppose $k$ has characteristic exponent $p$, and put $d = [k : k_0]$. Let $d' > 1$ be any integer which is prime to $pd$, and let $E_{/k_0}$ be any elliptic curve. By [ClSh, Thm. 3], there exists a field extension $l_0/k_0$ of degree $d'$ and a genus one curve $C_{/l_0}$ with Jacobian elliptic curve $E_{/l_0}$, such that $C$ is an element of $Ш(l_0, E)$ and has exact order $d'$. Let $A = \mathrm{Res}_{l_0/k_0} E$ and $W = \mathrm{Res}_{l_0/k_0} C$. Then $A_{/k_0}$ is an abelian variety of dimension $d_0$, and $W$ is a torsor under $A$ whose corresponding element of $H^1(k_0, A)$ is locally trivial and of order $d'$. Finally, consider $W_{/l}$: certainly it is locally trivial. On the other hand since $[l : k]$ is prime to $d'$, the cohomological restriction map $H^1(A, k_0)[d'] \to H^1(A, l)[d']$ is injective, so that $W(l) = \varnothing$. □

6.3. **Subvarieties of Varieties Violating HP.**

The construction of §6.2 can be made effective. The drawback is that $\dim W$ depends on $[l : k_0]$ and approaches infinity as $[l : k_0]$ becomes divisible by all sufficiently small primes. This leads us naturally to the following:

**Question.** *Let $k$ be a global field and $W_{/k}$ a nice variety which violates the Hasse Principle. Must there be a nice curve $C \subset_k W$ which violates the Hasse Principle?*

We will use the **fibration method** of Colliot-Thélène, Sansuc and Swinnerton-Dyer to show that the answer is *affirmative*. Combined with Theorem 13, this gives yet another construction of curves over any global field which violate HP.

We find it convenient to divide the proof into two parts: first we reduce to the case of surfaces, and then we apply the fibration method. (In so doing, we reduce to a situation in which we need the Riemann hypothesis for algebraic curves only, rather than for higher-dimensional varieties.)

**Theorem 14.** *Let $k$ be a global field and $W_{/k}$ a nice variety which violates HP, with $\dim W \geq 2$. Then there is a nice surface $S \subset_k W$ which violates HP.*

*Proof.* Step 1: Let $k$ be an infinite field, and let $W_{/k}$ a nice variety of dimension at least 2. Let $C \subset W$ be an nice curve which is a $k$-subscheme of $W$, and let $Z = \sum_i [P_i]$ be an effective $k$-rational zero-cycle with all the $P_i$'s distinct. Then there exists a closed subscheme $S \subset W$ which is a nice surface, and which contains both $C$ and the support of $Z$. Indeed, this is a direct consequence of the main result of [KA79].

Step 2: By Bertini's theorem, there is a nice curve $C \subset_k W$. Like any geometrically irreducible variety, $C$ can fail to have local points only at a finite set, say $S$, of places of $k$. Since $W$ has points everywhere locally, there exists an effective zero-cycle $Z_{/k}$ such that for all $v \in S$, $Z(k_v) \neq \varnothing$. Now we apply Step 1. □

**Theorem 15.** *Let $k$ be a global field and $S_{/k}$ a nice surface which violates HP. Then there is a nice curve $C \subset_k S$ which violates HP.*

*Proof.* Step 1: Let $\iota' : S \hookrightarrow \mathbb{P}^{N'}$ be any projective embedding, and let $\iota : S \to \mathbb{P}^N$ be the embedding obtained by composing $\iota'$ with the degree 3 Veronese embedding.

It follows from work of Katz [SGAVII, § XVII, Thm. 2.5] and Van de Ven [VdV, Theorem 1] that there exists a **strong Lefschetz pencil** for $\iota$, by which we mean a pencil $D = \{H_t\}$ of hyperplanes in $\mathbb{P}^N$ with the following properties:

(SLP1) The axis of $D$ cuts $S$ transversely.
(SLP2) For all $t$ in an open dense subset $U \subset D$, $H_t \cap S$ is a nice curve.
(SLP3) For every $t \in D$, $H_t \cap S$ is a geometrically integral curve with at worst ordinary double point singularities.

By blowing up the scheme-theoretic intersection of $S$ and the axis of $D$, we get a proper, flat morphism $\pi : \tilde{S} \to \mathbb{P}^1$ whose fiber over $t$ is isomorphic to $H_t \cap S$. By the Lang-Nishimura theorem [La54], [Ni], $\tilde{S}$ also violates HP. Since all but finitely many fibers give nice curves on $S$, it is enough to show that there are infinitely many fibers of $\pi$ which have points everywhere locally.

Step 2 (fibration method): We claim that there exists a finite set $S \subset \tilde{\Sigma}_k$, containing all the infinite places (by which we mean the Archimedean places in the number field case and the places over the point at $\infty$ in the function field case) such that for all $v \in \tilde{\Sigma}_k \setminus S$ and all $t \in \mathbb{P}^1(k)$, the fiber $\pi_t$ of $\pi$ over $t$ has a $k_v$-rational point.

Indeed, as is observed in [CTP, Lemma 3.1], by combining Theorem 11.1.1 and Theorem 12.2.4(viii) of [EGAIV], there exists a finite set of places $S$ of $k$, such that if $R$ is the ring of $S$-integers of $k$, then $\pi$ extends to a proper, flat morphism $\Pi : \tilde{\mathcal{S}} \to \mathbb{P}^1_{/R}$ all of whose fibers are geometrically integral. Because of the flatness, if $g$ is the genus of the fiber of $\pi$ at the generic point of $\mathbb{P}^1_{/K}$, for every $v \in \tilde{\Sigma}_k \setminus S$ and $t \in \mathbb{P}^1(K) = \mathbb{P}^1(R)$, the fiber over $(t, v)$ is a projective, geometrically integral curve of genus $g$ over the finite field $\mathbb{F}_v$. By comparing with the normalization and noting that the number of singular points can be bounded in terms of $g$, it follows from the Weil bounds that for all sufficiently large $v$ the fiber over $(t, v)$ has smooth $\mathbb{F}_v$-rational points. The claim now follows from Hensel's Lemma.

Step 3: For each $v \in S$, we have by assumption that $\tilde{S}(k_v) \neq \varnothing$, and accordingly $\pi(\tilde{S})(k_v)$ contains a nonempty $k_v$-analytically open subset $U_v$ of $\mathbb{P}^1(k_v)$. By weak approximation, there exists $t \in \mathbb{P}^1(k)$ such that $t \in U_v$ for all $v \in S$ and such that the fiber $\pi_t$ is smooth. By construction, $\pi_t$ has points everywhere locally. □

## References


[ACGH] E. Arbarello, M. Cornalba, P.A. Griffiths and J. Harris. *J. Geometry of algebraic curves.* Vol. I. Grundlehren der Mathematischen Wissenschaften, 267. Springer-Verlag, New York, 1985.

[BLM] A. Bremner, D.J. Lewis and P. Morton, *Some varieties with points only in a field extension.* Arch. Math. (Basel) 43 (1984), no. 4, 344–350.

[Bo] R. Bölling, *Die Ordnung der Schafarewitsch-Tate Gruppe kahn beliebig groβ werden*, Math. Nachr. 67 (1975), 157–179.

[Ca] J.W.S. Cassels, *Arithmetic on curves of genus 1. VI. The Tate-Safarevic group can be arbitrarily large*, J. Reine Angew. Math. 214/215 (1964), 65–70.

[Cl08] P.L. Clark, *An "anti-Hasse principle" for prime twists.* Int. J. Number Theory 4 (2008), no. 4, 627–637.

[ClSh] P.L. Clark and S. Sharif, *Period, index and potential sha*, submitted for publication.

[CM] D. Coray and C. Manoil, *On large Picard groups and the Hasse principle for curves and K3 surfaces*. Acta Arith. 76 (1996), no. 2, 165–189.

[CTP] J.-L. Colliot-Thélène and B. Poonen, *Algebraic families of nonzero elements of Shafarevich-Tate groups*. J. Amer. Math. Soc. 13 (2000), no. 1, 83–99.

[EGAIV] A. Grothendieck, *Éléments de géométrie algébrique. IV. 'Etude locale des schémas et des morphismes de schémas. III.* Inst. Hautes Études Sci. Publ. Math. No. 28 1966.

[Fis] T. Fisher, *Some examples of 5 and 7 descent for elliptic curves over* $\mathbb{Q}$, J. Eur. Math. Soc. 3 (2001), 169–201.

[Ge86] E.-U. Gekeler, *Über Drinfeldsche Modulkurven vom Hecke-Typ*. Compositio Math. 57 (1986), no. 2, 219–236.

[Ge01] E.-U. Gekeler, *Invariants of some algebraic curves related to Drinfeld modular curves*. J. Number Theory 90 (2001), no. 1, 166–183.

[KA79] S.L. Kleiman and A.B. Altman, *Bertini theorems for hypersurface sections containing a subscheme*. Comm. Algebra 7 (1979), no. 8, 775–790.

[La54] S. Lang, *Some applications of the local uniformization theorem*. Amer. J. Math. 76 (1954), 362–374.

[La87] S. Lang, *Elliptic functions*. With an appendix by J. Tate. Second edition. Graduate Texts in Mathematics, 112. Springer-Verlag, New York, 1987.

[Ma06] K. Matsuno, *Elliptic curves with large Shafarevich-Tate groups*. Trends in Mathematics, Information Center for Mathematical Sciences, Volume 9, Number 1, June, 2006, 49–53.

[Ma07] K. Matsuno, *Construction of elliptic curves with large Iwasawa* $\lambda$*-invariants and large Tate-Shafarevich groups*. Manuscripta Math. 122 (2007), no. 3, 289–304.

[MR] B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, preprint, April 2009.

[Me] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*. Invent. Math. 124 (1996), no. 1-3, 437–449.

[Ni] H. Nishimura, *Some remarks on rational points*. Mem. Coll. Sci. Univ. Kyoto. Ser. A. Math. 29 1955 189–192.

[Po04] B. Poonen, *Bertini theorems over finite fields*. Ann. of Math. (2) 160 (2004), no. 3, 1099–1127.

[Po07] B. Poonen, *Gonality of modular curves in characteristic p*. Math. Res. Lett. 14 (2007), no. 4, 691–701.

[Po09] B. Poonen, *Curves over every global field violating the local-global principle*. Preprint, http://www-math.mit.edu/∼poonen/papers/hasse_violation.pdf.

[Sa] P. Samuel, *Compléments à un article de Hans Grauert sur la conjecture de Mordell*. Inst. Hautes Études Sci. Publ. Math. No. 29 (1966), 55–62.

[Se] J.-P. Serre, *Topics in Galois theory*. Lecture notes prepared by Henri Damon. With a foreword by Darmon and the author. Research Notes in Mathematics, 1. Jones and Bartlett Publishers, Boston, MA, 1992.

[SGAVII] Groupes de monodromie en géométrie algébrique. II. (French) Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 II). Dirigé par P. Deligne et N. Katz. Lecture Notes in Mathematics, Vol. 340. Springer-Verlag, Berlin-New York, 1973.

[Sz] L. Szpiro, *Séminaire sur les Pinceaux de Courbes de Genre au Moins Deux*. Astérisque, 86. Société Mathématique de France, Paris, 1981.

[VdV] A. Van de Ven, *On the* 2*-connectedness of very ample divisors on a surface*. Duke Math. J. 46 (1979), 403–407.

[Wa] W.C. Waterhouse, *Abelian varieties over finite fields*. Ann. Sci. École Norm. Sup. (4) 2 (1969), 521–560.

Department of Mathematics,, University of Georgia,, Athens, GA 30602-7403, USA.
*E-mail address*: pete@math.uga.edu