Curves over every global field violating the local-global principle

| Citation       | Poonen, B. “Curves over Every Global Field Violating the Local-global Principle.” Journal of Mathematical Sciences 171.6 (2010): 782–785. Web. 27 Apr. 2012. © 2010 Springer Science+Business Media B.V. |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| As Published   | http://dx.doi.org/10.1007/s10958-010-0182-9                                                                                                                                                        |
| Publisher      | Springer-Verlag                                                                                                                                                                                   |
| Version        | Author’s final manuscript                                                                                                                                                                         |
| Citable link   | http://hdl.handle.net/1721.1/70470                                                                                                                                                                |
| Terms of Use   | Creative Commons Attribution-Noncommercial-Share Alike 3.0                                                                                                                                       |
| Detailed Terms | http://creativecommons.org/licenses/by-nc-sa/3.0/                                                                                                                                                |
CURVES OVER EVERY GLOBAL FIELD VIOLATING THE LOCAL-GLOBAL PRINCIPLE

BJORN POONEN

Abstract. There is an algorithm that takes as input a global field \( k \) and produces a curve over \( k \) violating the local-global principle. Also, given a global field \( k \) and a nonnegative integer \( n \), one can effectively construct a curve \( X \) over \( k \) such that \( \#X(k) = n \).

1. Introduction

Let \( k \) be a global field, by which we mean a finite extension of either \( \mathbb{Q} \) or \( \mathbb{F}_p(t) \) for some prime \( p \). Let \( \Omega_k \) be the set of nontrivial places of \( k \). For each \( v \in \Omega_k \), let \( k_v \) be the completion of \( k \) at \( v \). By variety, we mean a separated scheme of finite type over a field. A curve is a variety of dimension 1. Call a variety nice if it is smooth, projective, and geometrically integral. Say that a \( k \)-variety \( X \) satisfies the local-global principle if the implication

\[
X(k_v) \neq \emptyset \text{ for all } v \in \Omega_k \implies X(k) \neq \emptyset
\]

holds.

Nice genus-0 curves (and more generally, quadrics in \( \mathbb{P}^n \)) satisfy the local-global principle: this follows from the Hasse-Minkowski theorem for quadratic forms. The first examples of varieties violating the local-global principle were genus-1 curves, such as the smooth projective model of \( 2y^2 = 1 - 17x^4 \), over \( \mathbb{Q} \), discovered by Lind [Lin40] and Reichardt [Rei42].

Our goal is to prove that there exist curves over every global field violating the local-global principle. We can also produce curves having a prescribed positive number of \( k \)-rational points. In fact, such examples can be constructed effectively:

Theorem 1.1. There is an algorithm that takes as input a global field \( k \) and a nonnegative integer \( n \), and outputs a nice curve \( X \) over \( k \) such that \( \#X(k) = n \) and \( X(k_v) \neq \emptyset \) for all \( v \in \Omega_k \).

Remark 1.2. For the sake of definiteness, let us assume that \( k \) is presented by giving the minimal polynomial for a generator of \( k \) as an extension of \( \mathbb{Q} \) or \( \mathbb{F}_p(t) \). The output can be described by giving a finite list of homogeneous polynomials that cut out \( X \) in some \( \mathbb{P}^n \). For more details on representation of number-theoretic and algebraic-geometric objects, see [Len92, §2] and [BGJGP05, §5].

Date: May 14, 2010.

2000 Mathematics Subject Classification. Primary 11G30; Secondary 14H25.

Key words and phrases. Hasse principle, local-global principle, Dem'janenko-Manin method.

This research was supported by NSF grant DMS-0841321.
2. Proof

Lemma 2.1. Given a global field \( k \), one can effectively construct a nice curve \( Z \) over \( k \) such that \( Z(k) \) is finite, nonempty, and computable.

Proof. First suppose that \( \text{char } k = 0 \). Let \( E \) be the elliptic curve \( X_1(11) \) over \( k \). By computing a Selmer group, compute an integer \( r \) strictly greater than the rank of the finitely generated abelian group \( E(k) \). Let \( Z = X_1(11^r) \) over \( k \). By [DS03, Theorem 6.6.6], the Jacobian \( J_Z \) of \( Z \) is isogenous to a product of \( E^r \) with another abelian variety over \( k \) (geometrically, these \( r \) copies of \( E \) in \( J_Z \) arise from the degeneracy maps \( Z \to E \) indexed by \( s \in \{1, \ldots, r\} \) that in moduli terms send \( (A, P) \) to \( (A/(11^sP), 11^{s-1}P) \) where \( A \) is an elliptic curve and \( P \) is a point on \( A \) of exact order \( 11^r \)). So the Dem’janenko-Manin method [Dem66, Man69] yields an upper bound on the height of points in \( Z(k) \). In particular, \( Z(k) \) is finite and computable. It is also nonempty, since the cusp \( \infty \) on \( X_1(11^r) \) is a rational point.

If \( \text{char } k > 0 \), let \( Z \) be any nonisotrivial curve of genus greater than 1 such that \( Z(k) \) is nonempty: for instance, let \( a \) be a transcendental element of \( k \), and use the curve \( C_a \) in the first paragraph of the proof of Theorem 1.4 in [PP08]. Then \( Z(k) \) is finite by [Sam66, Théorème 4], and computable because of the height bound proved in [Szp81, §8, Corollaire 2]. □

Lemma 2.2. Given a global field \( k \) and a nonnegative integer \( n \), one can effectively construct a nice curve \( Y \) over \( k \) such that \( Y(k) \) is finite, computable, and of size at least \( n \).

Proof. Construct \( Z \) as in Lemma 2.1. Let \( \kappa(Z) \) denote the function field of \( Z \). Find a closed point \( P \in Z - Z(k) \) whose residue field is separable over \( k \).

If \( \text{char } k = 0 \), the Riemann-Roch theorem, which can be made constructive, together with a little linear algebra, lets us find \( f \in \kappa(Z) \) taking the value 1 at each point of \( Z(k) \), and having a simple pole at \( P \). If \( \text{char } k = p > 2 \), instead find \( t \in \kappa(Z) \) such that \( t \) has a pole at \( P \) and nowhere else, and such that \( t \) takes the value 1 at each point of \( Z(k) \); then let \( f = t + g^p \) for some \( g \in \kappa(Z) \) such that \( g \) has a pole at \( P \) of odd order greater than the order of the pole of \( t \) at \( P \) and no other poles, such that \( g \) is zero at each point of \( Z(k) \), and such that \( t + g^p \) is nonzero at each zero of \( dt \); this ensures that \( f \) has an odd order pole at \( P \) and no other poles, and is 1 at each point of \( Z(k) \), and has only simple zeros (since \( f \) and \( df = dt \) do not simultaneously vanish). In either case, \( f \) has an odd order pole at \( P \), so \( \kappa(Z)(\sqrt{T}) \) is ramified over \( \kappa(Z) \) at \( P \), so the regular projective curve \( Y \) with \( \kappa(Y) = \kappa(Z)(\sqrt{T}) \) is geometrically integral. A local calculation shows that \( Y \) is also smooth, so \( Y \) is nice. Equations for \( Y \) can be computed by resolving singularities of an initial birational model. The points in \( Z(k) \) split in \( Y \), so \( \#Y(k) = 2\#Z(k) \), and \( Y(k) \) is computable. Iterating this paragraph eventually produces a curve \( Y \) with enough points.

If \( \text{char } k = 2 \), use the same argument, but instead adjoin to \( \kappa(Z) \) a solution \( \alpha \) to \( \alpha^2 - \alpha = f \), where \( f \in \kappa(Z) \) has a pole of high odd order at \( P \), no other poles, and a zero at each point of \( Z(k) \).

□

Proof of Theorem 1.1. Given \( k \) and \( n \), apply Lemma 2.2 to find \( Y \) over \( k \) with \( Y(k) \) finite, computable, and of size at least \( n + 4 \). Write \( Y(k) = \{y_1, \ldots, y_m\} \). Find a closed point \( P \in Y - Y(k) \) with residue field separable over \( k \).

Suppose that \( \text{char } k \neq 2 \). Compute \( a, b \in k^\times \) whose images in \( k^\times/k^\times_2 \) are \( \mathbb{F}_2 \)-independent. Let \( S \) be the set of places \( v \in k \) such that \( a, b, \) and \( ab \) are all nonsquares in \( k_v \). By Hensel’s
lemma, if \( v \mid 2, \infty \) and \( v(a) = v(b) = 0 \), then \( v \notin S \). So \( S \) is finite and computable. Let \( w \in \Omega_k - S \). Weak approximation \([\text{AW43}] \) Theorem 1\], whose proof is constructive, lets us find \( c \in k^\times \) such that \( c \) is a square in \( k_v \) for all \( v \in S \) and \( w(c) \) is odd. The purpose of \( w \) is to ensure that \( c \) is not a square in \( k \). Find \( f \in \kappa(Y)^\times \) such that \( f \) has an odd order pole at \( P \) and a simple zero at each of \( y_1, \ldots, y_n \), and such that \( f(y_{n+1}) = a, f(y_{n+2}) = b, f(y_{n+3}) = ab, \) and \( f(y_{n+4}) = \cdots = f(y_m) = c \). If \( \text{char} \ k = p > 2 \), the same argument as in the proof of Lemma 2.2 lets us arrange in addition that \( f \) has no poles other than \( P \), and that all zeros of \( f \) are simple. Construct the nice curve \( X \) whose function field is \( \kappa(Y)(\sqrt{f}) \). Then \( X \to Y \) maps \( X(k) \) bijectively to \( \{y_1, \ldots, y_n\} \), so \( X(k) \) is computable and of size \( n \). Also, for each \( v \in \Omega_k \), at least one of \( a, b, ab, c \) is a square in \( k_v \), so \( X(k_v) \neq \emptyset \).

If \( \text{char} \ k = 2 \), use the same argument, with the following modifications. For any extension \( L \) of \( k \), define the additive homomorphism \( \varphi: L \to L \) by \( \varphi(t) = t^2 - t \). Construct \( a, b \in k \) such that the images of \( a \) and \( b \) in \( k/\varphi(k) \) are \( \mathbb{F}_2 \)-independent. Let \( S \) be the set of places \( v \in k \) such that \( a, b, \) and \( a + b \) are all outside \( \varphi(k_v) \). As before, \( S \) is finite and computable. Choose \( w \in \Omega_k - S \). Use weak approximation to find \( c \in k \) such that \( c \in \varphi(k_v) \) for all \( v \in S \) but \( c \notin \varphi(k_w) \). Find \( f \in \kappa(Y) \) such that \( f \) has a pole of high odd order at \( P \), a simple pole at \( y_1, \ldots, y_n \), and no other poles, and such that \( f(y_{n+1}) = a, f(y_{n+2}) = b, f(y_{n+3}) = a + b, \) and \( f(y_{n+4}) = \cdots = f(y_m) = c \). Construct the nice curve \( X \) whose function field is obtained by adjoining to \( \kappa(Y) \) a solution \( \alpha \) to \( \alpha^2 - \alpha = f \).

\[\square\]

3. Other constructions of curves violating the local-global principle

3.1. Lefschetz pencils in a Châtelet surface. J.-L. Colliot-Thélène has suggested another approach to constructing curves violating the local-global principle, which we now sketch. For any global field \( k \), there exists a Châtelet surface over \( k \) violating the local-global principle: see [Poo09, Proposition 5.1] and [Vir09, Theorem 1.1]. Let \( V \) be such a surface. Choose a projective embedding of \( V \). By [Kat73, Théorème 2.5], after replacing \( V \) by a \( d \)-uple embedding for some \( d \geq 1 \), there is a Lefschetz pencil of hyperplane sections of \( V \), fitting together into a family \( V \to \mathbb{P}^1 \), where \( V \) is the blowup of \( V \) along the intersection of \( V \) with the axis of the pencil. Since \( V \to V \) is a birational morphism, the Lang-Nishimura theorem (see [Nis55], [Lan54, Theorem 3], and also [CTCS80, Lemme 3.1.1]) shows that \( V \) has a \( k \)-point if and only if \( V \) does, and the same holds with \( k \) replaced by any completion \( k_v \). By definition of Lefschetz pencil, each geometric fiber of the pencil is either an integral curve or a union of two nice curves intersecting transversely in a single point. By requiring \( d \geq 3 \) above, we can ensure that each geometric fiber is also \( 2 \)-connected, which means that whenever it decomposed as a sum \( D_1 + D_2 \) of two nonzero effective divisors, the intersection number \( D_1.D_2 \) is at least \( 2 \) (the \( 2 \)-connectedness follows from [VdV79, Theorem 1]; that paper is over \( \mathbb{C} \), but the argument works in arbitrary characteristic). This rules out the possibility of a geometric fiber with two components, so every geometric fiber is integral. The “fibration method” (see, e.g., [CTSSD87], [CT98 2.1], [CTP00, Lemma 3.1]) shows that there is a finite set of places \( S \) such that for every place \( v \notin S \) and every point \( t \in \mathbb{P}^1(k) \), the fiber of \( V \to \mathbb{P}^1 \) above \( t \) has a \( k_v \)-point. For \( v \in S \), the set \( V(k_v) \) is nonempty, and its image in \( \mathbb{P}^1 \) contains a nonempty open subset \( U_v \) of \( \mathbb{P}^1(k_v) \). By weak approximation, we can find \( t \in \mathbb{P}^1(k) \) such that \( t \in U_v \) for all \( v \in S \), and such that the fiber of \( V \to \mathbb{P}^1 \) above \( t \) is smooth. That fiber violates the local-global principle.
With a little work, this construction can be made effective. On the other hand, this approach does not seem to let one construct curves with a prescribed positive number of points.

3.2. Atkin-Lehner twists of modular curves. Theorem 1 of [Cla08] constructs a natural family of curves over \(\mathbb{Q}\) violating the local-global principle: namely, for any squarefree integer \(N\) with \(N > 131\) and \(N \neq 163\), there is a positive-density set of primes \(p\) such that the twist of \(X_0(N)\) by the main Atkin-Lehner involution \(w_N\) and the quadratic extension \(\mathbb{Q}(\sqrt{p})/\mathbb{Q}\) violates the local-global principle over \(\mathbb{Q}\). See [Cla08] for details, and for a connection to the inverse Galois problem. The proof involves Faltings’ theorem [Fal83], so it does not yield an effective construction of a suitable pair \((N, p)\).

On the other hand, as P. Clark explained to me, a variant of this construction is effective, and works over an arbitrary global field \(k\). His idea is to replace \(X_0(N)\) above with a modular curve \(X\) having both \(\Gamma_0(N)\) and \(\Gamma_1(M)\) level structures, for suitable \(M\) and \(N\) depending on \(k\), and to apply Merel’s theorem (or a characteristic \(p\) analogue) to \(X_1(M)\) to control \(X(k)\). See [Cla09] for details.

Remark 3.1. One can also find counterexamples to the local-global principle over \(\mathbb{Q}\) among Atkin-Lehner quotients of Shimura curves: see [RSY05] and [PY07].

Acknowledgements
I thank Pierre Dèbes for the suggestion to use the Dem’janenko-Manin method. I thank Pete L. Clark and Jean-Louis Colliot-Thélène for sharing their ideas sketched in Section 3. I also thank Clark for a correction, and Izzet Coskun for suggesting the reference [VdV79]. Finally I thank the referee for a few suggestions.

References

[AW45] Emil Artin and George Whaples, Axiomatic characterization of fields by the product formula for valuations, Bull. Amer. Math. Soc. 51 (1945), 469–492. MR 0013145 (7,111f)

[BGJGP05] Matthew H. Baker, Enrique González-Jiménez, Josep Gonzáles, and Bjorn Poonen, Finiteness results for modular curves of genus at least 2, Amer. J. Math. 127 (2005), 1325–1387. arXiv:math.NT/0211394.

[Cla08] Pete L. Clark, An “anti-Hasse principle” for prime twists, Int. J. Number Theory 4 (2008), no. 4, 627–637. MR 2441796

[Cla09] ______, Curves over global fields violating the Hasse principle: some systematic constructions, May 21, 2009. Preprint, arXiv:0905.3459, to appear in IMRN.

[CT98] J.-L. Colliot-Thélène, The Hasse principle in a pencil of algebraic varieties, Number theory (Tiruchirapalli, 1996), Contemp. Math., vol. 210, Amer. Math. Soc., Providence, RI, 1998, pp. 19–39. MR 1478483 (98g:11075)

[CTCS80] Jean-Louis Colliot-Thélène, Daniel Coray, and Jean-Jacques Sansuc, Descente et principe de Hasse pour certaines variétés rationnelles, J. reine angew. Math. 320 (1980), 150–191 (French). MR 592151 (82f:14020)

[CTP00] Jean-Louis Colliot-Thélène and Bjorn Poonen, Algebraic families of nonzero elements of Shafarevich-Tate groups, J. Amer. Math. Soc. 13 (2000), no. 1, 83–99. MR1697093 (2000f:11067)

[CTSSD87] Jean-Louis Colliot-Thélène, Jean-Jacques Sansuc, and Peter Swinnerton-Dyer, Intersections of two quadrics and Châtelet surfaces. I, J. reine angew. Math. 373 (1987), 37–107. MR 870307 (88m:11045a)
