Записки научных
семинаров ПОМИ
Том 377, 2010 г.

B. Poonen

CURVES OVER EVERY GLOBAL FIELD VIOLATING THE LOCAL-GLOBAL PRINCIPLE

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 Ω_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

$$X(k_v) \neq \varnothing \quad \text{for all} \quad v \in \Omega_k \implies X(k) \neq \varnothing$$

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 [15] and Reichardt [21].

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 $X(k_v) \neq \varnothing$ for all $v \in \Omega_k$.*

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

This research was supported by NSF grant DMS-0841321.

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 [14, §2] and [2, §5].

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 $\operatorname{char} k = 0$. 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 [10, 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 $s \in \{1, \dots, r\}$ that in moduli terms send (A, P) to $(A/\langle 11^s P\rangle, 11^{s-1}P)$ where A is an elliptic curve and P is a point on A of exact order 11^r). So the Dem'janenko–Manin method [9, 16] 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 ∞ on $X_1(11^r)$ is a rational point.

If $\operatorname{char} k > 0$, 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 [20]. Then $Z(k)$ is finite by [23, Théorème 4], and computable because of the height bound proved in [24, §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 $\operatorname{char} k = 0$, 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 $\operatorname{char} k = p > 2$, 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 $\kappa(Z)(\sqrt{f})$ is ramified over $\kappa(Z)$ at P, so the regular projective curve Y with $\kappa(Y) = \kappa(Z)(\sqrt{f})$ 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 $\operatorname{char} k = 2$, use the same argument, but instead adjoin to $\kappa(Z)$ a solution α 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 to find Y over k with $Y(k)$ finite, computable, and of size at least $n + 4$. Write $Y(k) = \{y_1, \dots, y_m\}$. Find a closed point $P \in Y - Y(k)$ with residue field separable over k.

Suppose that $\operatorname{char} k \neq 2$. 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 $v \nmid 2, \infty$ and $v(a) = v(b) = 0$, then $v \notin S$. So S is finite and computable. Let $w \in \Omega_k - S$. Weak approximation [1, 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 $y_1, \dots, y_n$, 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 $\operatorname{char} k = p > 2$, 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 $\{y_1, \dots, y_n\}$, 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 $X(k_v) \neq \varnothing$.

If $\operatorname{char} k = 2$, use the same argument, with the following modifications. For any extension L of k, define the additive homomorphism $\mathfrak{p}\colon L \to L$ by $\mathfrak{p}(t) = t^2 - t$. Construct $a, b \in k$ such that the images of a and b in

$k/\mathfrak{p}(k)$ 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 $\mathfrak{p}(k_v)$. As before, S is finite and computable. Choose $w \in \Omega_k - S$. Use weak approximation to find $c \in k$ such that $c \in \mathfrak{p}(k_v)$ for all $v \in S$ but $c \notin \mathfrak{p}(k_w)$. Find $f \in \kappa(Y)$ such that f has a pole of high odd order at P, a simple pole at $y_1, \dots, y_n$, 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 α to $\alpha^2 - \alpha = f$. □

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 [19, Proposition 5.1] and [26, Theorem 1.1]. Let V be such a surface. Choose a projective embedding of V. By [12, Théorème 2.5], after replacing V by a d-uple embedding for some $d \geqslant 1$, there is a Lefschetz pencil of hyperplane sections of V, fitting together into a family $\widetilde{V} \to \mathbb{P}^1$, where $\widetilde{V}$ is the blowup of V along the intersection of V with the axis of the pencil. Since $\widetilde{V} \to V$ is a birational morphism, the Lang–Nishimura theorem (see [17], [13, Theorem 3], and also [6, Lemme 3.1.1]) shows that $\widetilde{V}$ 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 $d \geqslant 3$ 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 [25, Theorem I]; 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., [8], [5, 2.1], [7, 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 $\widetilde{V} \to \mathbb{P}^1$ above t has a k_v-point. For $v \in S$, the set $\widetilde{V}(k_v)$ 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 $\widetilde{V} \to \mathbb{P}^1$ 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 [3] 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 [3] for details, and for a connection to the inverse Galois problem. The proof involves Faltings' theorem [11], 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 [4] 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 [5] and [18].

Acknowledgments

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 Sec. 3. I also thank Clark for a correction, and Izzet Coskun for suggesting the reference [25]. Finally I thank the referee for a few suggestions.

References

1. E. Artin, G. Whaples, *Axiomatic characterization of fields by the product formula for valuations.* — Bull. Amer. Math. Soc. **51**, (1945), 469–492,
2. M. H. Baker, E. González-Jiménez, J. González, B, Poonen, *Finiteness results for modular curves of genus at least* 2. — Amer. J. Math. **127**, (2005), 1325–1387.
3. P. L. Clark, *An "anti-Hasse principle" for prime twists.* — Int. J. Number Theory **4** (2008), 627–637,
4. P. L. Clark, *Curves over global fields violating the Hasse principle: some systematic constructions.* Preprint, `arXiv:0905.3459`, to appear in IMRN, 2009-05-21.

5. J.-I. Colliot-Thélène, *The Hasse principle in a pencil of algebraic varieties.* — In: Number theory, (Tiruchirapalli 1996), Contemp. Math., **210**, Amer. Math. Soc., Providence, RI (1998), pp. 19–39.
6. J.-I. Colliot-Thélène, D. Daniel, J.-J. Sansuc, *Descente et principe de Hasse pour certaines variétés rationnelles.* — J. reine angew. Math. **320** (1980), 150–191.
7. J.-I. Colliot-Thélène, B. Bjorn, *Algebraic families of nonzero elements of Shafarevich–Tate groups.* — J. Amer. Math. Soc. **13** (2000), No. 1, 83–99.
8. J.-I. Colliot-Thélène, J.-J. Sansuc, P. Swinnerton-Dyer, *Intersections of two quadrics and Châtelet surfaces. I.* — J. reine angew. Math. **373** (1987), 37–107.
9. В. А. Демьяненко, *Рациональные точки одного класса алгебраических кривых.* — Изв. АН СССР, сер. матем. **30**:6 (1966), 1373–1396. V. A. Dem'janenko, *Rational points of a class of algebraic curves.* — Izv. Akad. Nauk SSSR, Ser. Mat. [Russian] **30** (1966), 1373–1396.
   Translation in *Thirteen papers on group theory, algebraic geometry, and algebraic topology* — American Mathematical Society Translations, series 2 **66**, Providence, RI (1967), 246–272.
10. F. Diamond, J. Shurman, *A first course in modular forms.* — Graduate Texts in Mathematics **228**, Springer-Verlag, New York 2005 xvi+436.
11. G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* — Invent. Math. **73** (1983), No. 3., 349–366.
12. N. M. Katz, *Pinceaux de Lefschetz: théorème d'existence.* — Lect. Notes Math. **340**, Exposé XVII, Springer-Verlag, Berlin (1973), 212–253.
13. S. Lang, *Some applications of the local uniformization theorem.* — Amer. J. Math. **76** (1954), 362–374.
14. H. W. Lenstra Jr., *Algorithms in algebraic number theory.* — Bull. Amer. Math. Soc. (N.S.) **26** (1992), No. 2 211–244.
15. C.-E. Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins.* — Thesis, University of Uppsala **1940**, 1940, 97.
16. Ю. И.. Манин, *p-кручение эллиптических кривых равномерно ограничено.* — Изв. АН СССР, сер. матем. **33**:6 (1969), 459–465. Yu. I. Manin, *The p-torsion of elliptic curves is uniformly bounded.* — Izv. Akad. Nauk SSSR Ser. Mat. [Russian] **33** (1969), 459–465. Translation in *Mathematics of the USSR-Izvestiya* **3**, No. 3 (1969), 433–438.
17. H. Nishimura, *Some remarks on rational points.* — Mem. Coll. Sci. Univ. Kyoto, Ser. A. Math. **29** (1955), 189–192.
18. P. Parent, A. Yafaev, *Proving the triviality of rational points on Atkin–Lehner quotients of Shimura curves.* — Math. Ann. **339** (2007), No. 4, 915–935.
19. B. Poonen, *Existence of rational points on smooth projective varieties.* — J. Eur. Math. Soc. (JEMS) **11** (2009), No. 3, 529–543.
20. B. Poonen, F. Pop, *First-order characterization of function field invariants over large fields.* — In: Model theory with applications to algebra and analysis. Vol. 2, London Math. Soc. Lect. Note Ser. **350**, Cambridge Univ. Press, Cambridge (2008), pp. 255–271.
21. H. Reichardt, *Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen.* — J. reine angew. Math. **184** (1942), 12–18.

22. V. Rotger, A. Skorobogatov, A. Yafaev, *Failure of the Hasse principle for Atkin–Lehner quotients of Shimura curves over* $\mathbb{Q}$. — Mosc. Math. J. **5** (2005), No. 2, 463–476, 495.
23. P. Samuel, *Compléments à un article de Hans Grauert sur la conjecture de Mordell*. — Inst. Hautes Études Sci. Publ. Math. **29**, (1966), 55–62.
24. L. Szpiro, *Propriétés numériques du faisceau dualisant relatif*. — In: Séminaire sur les Pinceaux de Courbes de Genre au Moins Deux, Astérisque **86**, Société Mathématique de France (1981), pp. 44–78.
25. A. Van de Ven, *On the* 2*-connectedness of very ample divisors on a surface*. — Duke Math. J. **46** (1979), No. 2, 403–407.
26. B. Viray, *Failure of the Hasse principle for Châtelet surfaces in characteristic* 2. Preprint, `arXiv:0902.3644` 2009-10-12.

Department of Mathematics,
Massachusetts Institute of Technology,
Cambridge, MA 02139-4307, USA

E-mail: poonen@math.mit.edu

Поступило 14 мая 2010 г.