FINITE DESCENT OBSTRUCTION ON CURVES AND MODULARITY

DAVID HELM AND JOSÉ FELIPE VOLOCH

Abstract. We prove that a form of finite Galois descent obstruction is the only obstruction to the existence of S integral points on integral models of twists of modular curves over $\mathbf{Q}$, for any finite set of primes S. We deduce this from an existence theorem for elliptic curves over $\mathbf{Q}$ satisfying certain local conditions.

1. Introduction

Recent work on local-global principles for rational points on algebraic curves has been spurred by the question raised by Skorobogatov [11] and Scharaschkin [8] of whether the Brauer-Manin obstruction is the only obstruction to the existence of rational points. Bruin and Stoll [1] have provided extensive numerical evidence that the answer is yes and Poonen and the second author [7] proved this in the function field case. Also, Stoll [12] has looked at this question from the point of view of finite abelian descent obstructions and formulated a weaker conjecture in terms of finite Galois descent obstructions.

The purpose of this paper is to look at the analogue of these questions for integral points on affine curves. Harari and the second author [2] have studied local-global principles in this context, discussed the corresponding questions and showed the equivalence between various formulations of the finite abelian descent obstruction. In this paper, we look at the finite Galois descent obstruction for modular curves over $\mathbf{Q}$, relate it to a problem on the existence of elliptic curves satisfying certain local conditions and prove said existence over the rationals. As a consequence, the finite Galois descent obstruction is the only obstruction for the existence of S-integral points on integral models of modular curves over $\mathbf{Q}$, for an arbitrary finite set of primes S. The main technical tool to prove the existence of the elliptic curves alluded to above is Serre's conjectures [9] on Galois representations, recently proved by Khare and Wintenberger [5].

2000 *Mathematics Subject Classification.* Primary 11G30; Secondary 14G25.

Key words and phrases. descent obstruction, modularity, galois representation.

2. Descent theory

Let K be a field with algebraic closure $\overline{K}$. By *K-curve*, we always mean a smooth and geometrically integral finite type scheme of dimension 1 over $\operatorname{Spec} K$.

If X is a geometrically integral K-scheme, we set $\overline{X} = X \times_K \overline{K}$.

Let X be a smooth and geometrically integral scheme over a number field K. Let Ω_K be the set of all places of K. For a place v of K, we denote by K_v the corresponding completion and, if v is non-archimedean, $\mathcal{O}_v$ is its ring of integers.

From now on we assume that K is a number field. We fix a finite set S of "bad" places of K (including all archimedean places and all places of bad reduction of X) and we choose a smooth model $\mathcal{X}$ of X over the ring of S-integers $\mathcal{O}_S$.

Let $\pi : Y \to X$ be a map of curves such that $\pi : \overline{Y} \to \overline{X}$ is Galois. As usual, a twist of π is a map $\pi' : Y' \to X$ such that $\pi' : \overline{Y}' \to \overline{X}$ is isomorphic over $\bar{K}$ to $\pi : \overline{Y} \to \overline{X}$ as a cover. The set of isomorphism classes of twists of π will be denoted $Tw(\pi)$. Standard descent theory ([11]) gives the following:

$$\mathcal{X}(\mathcal{O}_S) = \cup_{\pi' \in Tw_0(\pi)} \pi'(\mathcal{Y}'(\mathcal{O}_S))$$

where $Tw_0(\pi)$ is a finite subset of $Tw(\pi)$. Indeed, for $P \in \mathcal{X}(\mathcal{O}_S)$, $\pi^{-1}(P)$ is a torsor of the Galois group of π which determines a π'. The set $Tw_0(\pi)$ is simply the set of all torsors obtained from such points P and its finiteness follows from the Chevalley-Weil theorem.

Let $(P_v) \in \prod_{v \notin S} \mathcal{X}(\mathcal{O}_v)$. If there exists $\pi' \in Tw_0(\pi)$ such that the twisted torsor $\mathcal{Y}'$ contains a point $(Q_v) \in \prod_{v \notin S} \mathcal{Y}'(\mathcal{O}_v)$ that maps to (P_v), we say that (P_v) is unobstructed by the cover. Global points are thus unobstructed. A natural question is to identify those adelic points that are unobstructed by all Galois covers which we denote by $\mathcal{X}^{f-cov}$ following [12].

Consider a (P_v) in $\mathcal{X}^{f-cov}$. By a *compatible system of lifts* of (P_v), we mean a choice, for each Galois cover $\pi : Y \to X$, of a twist $\pi' : Y' \to X$ of π, and a point $(P_v)_\pi$ of $\prod_{v \notin S} \mathcal{Y}'(\mathcal{O}_v)$ lifting (P_v), that are compatible in the following sense: if $\pi_1, \pi_2 : Y \to X$ are Galois covers, such that π_2 dominates π_1, then π_2' dominates π_1' and $(P_v)_{\pi_2'}$ maps to $(P_v)_{\pi_1'}$. It is clear that an $\mathcal{O}_S$-point of $\mathcal{X}$ admits a compatible system of lifts. We let $\mathcal{X}^{\infty-cov}$ denote the subset of $\mathcal{X}^{f-cov}$ consisting of those adelic points that admit a compatible system of lifts.

We thus have $\mathcal{X}(\mathcal{O}_S) \subset \mathcal{X}^{\infty-cov} \subset \mathcal{X}^{f-cov}$, but *a priori* it is possible for $\mathcal{X}^{\infty-cov}$ to be strictly smaller than $\mathcal{X}^{f-cov}$. We will show that this is not the case.

Lemma 2.1. *Let T be a rooted tree such that each of its vertices has only finitely many children, and such that T contains branches of arbitrarily large length. Then T contains an infinite branch.*

Proof. Let v_0 be the root of T. Then v_0 has finitely many children $w_1, \dots, w_n$. Let T_i be the subtree of T containing w_i and all of the descendants of w_i. As T has branches of arbitrary length, the same must be true for one of the T_i. Take $v_1 = w_i$. Similarly, take v_2 to be a child of v_1 such that the tree consisting of the descendants of v_2 has branches of arbitrarly length. Proceeding, we obtain an infinite branch $v_0, v_1, v_2, \dots$. □

Proposition 1. *Every (P_v) in $\mathcal{X}^{f-cov}$ admits a compatible system of lifts; that is, $\mathcal{X}^{\infty-cov} = \mathcal{X}^{f-cov}$.*

Proof. By [12], Lemma 5.7, there is a sequence of Galois covers Y_i of X, such that $Y_0 = X$, Y_{i+1} dominates Y_i for each i, and for any Galois cover Z of X, there is an i such that Y_i dominates Z. Let T be the tree whose vertices are pairs (i, Y_i'), where i is a nonnegative integer and Y_i' is a twist of Y_i such that (P_v) lifts to $\mathcal{Y}_i$. The children of a given (i, Y_i') are those pairs $(i+1, Y_{i+1}')$ such that Y_{i+1}' dominates Y_i'.

As (P_v) is in $\mathcal{X}^{f-cov}$, T has branches of arbitrarily large length. On the other hand, by [12], 5.1, there are only finitely many twists Y_i' of a given Y_i such that (P_v) lifts to Y_i'; thus each vertex of T has only finitely many children. By the Lemma, we thus have for each i a twist Y_i' of Y_i such that (P_v) lifts to Y_i', and Y_{i+1}' dominates Y_i'.

We now construct a sequence $(P_v)_i$ of lifts of (P_v) to Y_i' such that for all i, $(P_v)_{i+1}$ maps to $(P_v)_i$ under the map $Y_{i+1}' \to Y_i'$. Fix a place v, and consider the tree T_v whose vertices are pairs $(i, P_{v,i})$, where i is a nonnegative integer and $P_{v,i}$ is a lift of P_v to a K_v-point of Y_i'. An edge of T_v connects $(i, P_{v,i})$ with $(i+1, P_{v,i+1})$ if $P_{v,i+1}$ maps to $P_{v,i}$ under the map $Y_{i+1}' \to Y_i$. Then T_v has branches of arbitrarily large length, as (P_v) lifts to Y_i' for all i. On the other hand, each vertex has only finitely many children, as only finitely many K_v-points of Y_{i+1}' lie over a given point of Y_i'. We thus obtain an infinite branch of T_v; that is, a sequence of points $P_{v,i}$, compatible under the maps $Y_{i+1}'(K_v) \to Y_i'(K_v)$.

For each i, let the adelic point $(P_v)_i$ of Y_i' be the point obtained by taking the points $P_{v,i}$ for all v. It is now straightforward to extend the sequence $(P_v)_i$ to a compatible system of lifts of (P_v). If $Z \to X$ is a Galois cover, there exists a twist Z' of Z dominated by some Y_i'. We then attach to Z the pair $(Z', (P_v)_{Z'})$, where $(P_v)_{Z'}$ is the image of $(P_v)_i$ in Z'. It is clear that this does not depend on the choice of Y_i'. □

3. Modular curves

Let $Y_N/\mathbf{Q}$ be the affine curve parametrizing triples (E, P, C) where E is an elliptic curve, P is a point on E of exact order N and C is a cyclic subgroup of E of order N such that P and C generate $E[N]$. Y_N has a smooth model over $\mathbf{Z}[1/N]$. The set of twists of $\pi : Y_N \to Y_1$ over a field K correspond to the set of Galois representations $\rho : G_K \to GL_2(\mathbf{Z}/N)$ whose determinant is the cyclotomic character $\chi : G_K \to (\mathbf{Z}/N)^*$. This is proved in [6] and [10]. If E/K is an elliptic curve and the corresponding point of $Y_1(K)$ lifts to a K-rational point of the twist of Y_N corresponding to a representation ρ, then ρ describes the action of G_K on $E[N]$.

We will prove

Theorem 2. *Let $\mathcal{X}$ be the S-integral model of a twist of $X(m)$ corresponding to a representation $\rho : G_K \to GL_2(\mathbf{Z}/m)$. We have that, if $\mathcal{X}^{f-cov}$ is non-empty then for all $v \notin S$ there exists elliptic curves E_v/K_v with good reduction at v and, for all primes ℓ there exist Galois representations $\rho_\ell : G_K \to GL_2(\mathbf{Z}_\ell)$, whose determinant is the cyclotomic character, such that ρ_ℓ restricted to a decomposition group at v corresponds to the action of G_{K_v} on the Tate module $T_\ell E_v$, and that, for ℓ^a dividing m, the reduction modulo ℓ^a, $G_K \to GL_2(\mathbf{Z}/\ell^a)$ of ρ_ℓ is the representation induced by ρ.*

Proof. The S-integral points of $\mathcal{X}$ correspond to elliptic curves with good reduction outside S and and such that G_K acts on $E[m]$ via ρ.

Assume now that $\mathcal{X}^{f-cov}$ is non-empty and consider the covers $Y_N \to Y_m$ for N divisible by m. By lifting ρ to a representation to $GL_2(\mathbf{Z}/N)$, we obtain a cover of $\mathcal{X}$.

Fix a point (P_v) of $\mathcal{X}^{f-cov}$. Proposition 1 allows us to fix a compatible system of lifts of (P_v). In particular, for each N divisible by m we obtain a twist Y'_N of Y_N (corresponding to a representation $\rho_N : G_K \to GL_2(\mathbf{Z}/N)$ lifting ρ), and a compatible family of points $(P_v)_N$ of Y'_N lifting (P_v).

For N sufficiently large (indeed, $N \geq 3$ suffices), Y'_N is a fine moduli space of elliptic curves. The point $(P_v)_N$ thus yields, for each v, an elliptic curve E_v over K_v, with good reduction at v, and an isomorphism of the G_{K_v}-module $E_v[N]$ with the restriction of ρ_N to a decomposition group at v. The compatibility of the system $\{(P_v)_N\}$ guarantees that the E_v that arise in this way are independent of N.

Fix ℓ. For any positive integer a, the representation $\overline{\rho}_{\ell^a} : G_K \to GL_2(Z/\ell^a)$ obtained by reducing any ρ_N modulo ℓ^a (for ρ_N divisible by ℓ^a) is independent of N; the action of G_{K_v} on $E_v[\ell^a]$ is given by

the restriction of ρ_{ℓ^a} to a decomposition group at v. Let ρ_ℓ be the limit of the $\overline{\rho}_{\ell^a}$; it is then clear that the action of G_{K_v} on $T_\ell E_v$ is given by the restriction of ρ_ℓ to a decomposition group at v. The relationship between the reduction mod ℓ^a of ρ_ℓ and ρ is clear from the construction. □

Theorem 3. *Assume that $K = \mathbf{Q}$. Let $\mathcal{X}$ be the S-integral model of a twist of $X(m)$ corresponding to a representation $\rho : G_K \to GL_2(\mathbf{Z}/m)$. We have that, if $\mathcal{X}^{f-cov}$ is non-empty then $\mathcal{X}(\mathbf{Z}_S)$ is non-empty.*

Proof. We are in the situation of Theorem 2 and thus we have a collection of elliptic curves and Galois representations. We will prove (Theorem 4 in the next section) that, in the case $K = \mathbf{Q}$, the existence of such a collection of elliptic curves and Galois representations imply the existence of an elliptic curve $E/\mathbf{Q}$, with good reduction away from S and such that $G_{\mathbf{Q}}$ acts on $E[m]$ via ρ. Such an elliptic curve thus gives a point in $\mathcal{X}(\mathbf{Z}_S)$. □

In [12] Corollary 8.8, Stoll proves the analogue of Theorem 3 for rational points, under the additional hypotheses that $X(m)$ has positive genus and that ρ is the trivial representation, using the fact that the Jacobian of these curves have a factor with finite Mordell-Weil and Tate-Shafarevich groups. His result, combined with Theorem 3 of [2], implies the conclusion of Theorem 3 under the aforementioned additional hypotheses.

4. Serre's conjecture

Now restrict to the case $K = \mathbf{Q}$, and assume we are in the setting of Theorem 2; that is, we are given a finite set of rational primes S, and for each p outside S we have an elliptic curve $E_p/\mathbf{Q}_p$ with good reduction. Moreover, for all primes ℓ, there exists a Galois representation $\rho_\ell : G_{\mathbf{Q}} \to GL_2(\mathbf{Z}_\ell)$, such that for all p outside S, the action of $G_{\mathbf{Q}_p}$ on $T_\ell E_p$ is given by the restriction of ρ_ℓ to a decomposition group at p. Finally, we have an integer m, and a representation $\rho : G_Q \to GL_2(\mathbf{Z}/m)$, such that for all pairs ℓ, a such that ℓ^a divides m, the reductions of ρ_ℓ and ρ modulo ℓ^a agree.

Our goal is to show that such a collection of elliptic curves E_p gives rise to an elliptic curve E over $\mathbf{Q}$, with good reduction outside S. More precisely:

Theorem 4. *There exists an elliptic curve E over $\mathbf{Q}$, such that $T_\ell E$ is isomorphic to ρ_ℓ as representations of $G_{\mathbf{Q}}$ for all ℓ. In particular, E has good reduction at all p outside S and the action of of $G_{\mathbf{Q}}$ in $E[m]$ is given by ρ.*

We will construct E using the theory of modular forms. The key result that is necessary is Serre's conjecture [9] (now a theorem of Khare and Wintenberger [5].)

Theorem 5 (Serre's conjecture)**.** *Let $\overline{\rho} : G_{\mathbf{Q}} \to GL_2(\overline{\mathbf{F}}_\ell)$ be odd and absolutely irreducible. Then $\overline{\rho}$ arises from a classical modular eigenform of an explicit weight $k(\overline{\rho})$ and an explicit level $N(\overline{\rho})$.*

Serre gives concrete descriptions of the optimal weight $k(\overline{\rho})$ and the optimal level $N(\overline{\rho})$; in particular $N(\overline{\rho})$ is the prime-to-ℓ part of the Artin conductor of $\overline{\rho}$. The description of the optimal weight is in terms of the restriction of $\overline{\rho}$ to a decomposition group at ℓ, and is somewhat more complicated; we refer the reader to section 2 of [9] for details.

We are grateful to Tong Liu for explaining how the following result follows from Theorem 5; the key ideas are all already present in [9] (especially section 4.8).

Proposition 6. *For each p outside S, set $a_p = p+1-\#E_p(\mathbf{F}_p)$. There exists a normalized weight 2 classical modular eigenform f, with integer coefficients, such that for all p outside S, $a_p(f) = a_p$, where $a_p(f)$ is the p-th Fourier coefficient of f.*

Proof. For each prime ℓ, let $\overline{\rho}_\ell$ be the mod ℓ reduction of ρ_ℓ. We begin by constructing an infinite collection of ℓ_i such that $k(\overline{\rho}_{\ell_i})$ and $N(\overline{\rho}_{\ell_i})$ are bounded.

For ℓ outside S, the restriction of $\overline{\rho}_\ell$ to a decomposition group at ℓ gives the action of $G_{\mathbf{Q}_\ell}$ on the ℓ-torsion of E_ℓ. As E_ℓ has good reduction, its ℓ-torsion extends to a finite flat group scheme over $\mathbf{Z}_\ell$. Thus $\overline{\rho}_\ell$ is finite at ℓ; by [9], Proposition 4, we then have $k(\overline{\rho}_\ell) = 2$.

We now consider $N(\overline{\rho}_\ell)$, for ℓ outside S. As $\overline{\rho}_\ell$ is unramified outside $S \cup \ell$, $N(\overline{\rho}_\ell)$ is divisible only by primes in S. Moreover, by [9], Proposition 9, the valuation of $N(\overline{\rho}_\ell)$ at a prime p in S is bounded in terms of the order of $\overline{\rho}_\ell(W_p)$, where W_p is the wild inertia subgroup of a decomposition group at p.

The image $\overline{\rho}_\ell(W_p)$ is a p-group contained in $GL_2(\mathbf{F}_\ell)$; the latter has order $(\ell^2-1)(\ell^2-\ell)$. Thus, if ℓ satisfies the following congruence conditions:

- $\ell \not\equiv \pm 1 \pmod 8$,
- $\ell \not\equiv \pm 1$ 4, or 7 $\pmod 9$,
- $\ell \not\equiv \pm 1 \pmod p$ for all $p \in S$ other than 2 or 3,

then the order of $\overline{\rho}_\ell(W_2)$ divides 2^5, the order of $\overline{\rho}_\ell(W_3)$ divides 3, and the order of $\overline{\rho}_\ell(W_p)$ is trivial for all other p. By [9], Proposition 9 and its corollary, it then follows that for ℓ satisfying these congruence conditions, one has:

- $\mathrm{ord}_2(N(\overline{\rho}_\ell)) \leq 14$,
- $\mathrm{ord}_3(N(\overline{\rho}_\ell)) \leq 5$, and
- $\mathrm{ord}_p(N(\overline{\rho}_\ell)) \leq 2$ for $p \in S$ other than 2 or 3.

In other words, $N(\overline{\rho}_\ell)$ divides N, where $N = 2^{14}3^5p_1^2, \ldots, p_r^2$, and $p_1, \ldots, p_r$ are the primes in S other than 2 and 3.

We next show that for all but finitely many of the ℓ satisfying the above congruences, $\overline{\rho}_\ell$ is absolutely irreducible. If ℓ is not in S, and E_ℓ has supersingular reduction, and so the action of $G_{\mathbf{Q}_\ell}$ on $E_\ell[\ell]$ is absolutely irreducible. Thus in such cases $\overline{\rho}_\ell$ is absolutely irreducible.

Suppose now that there are infinitely many ℓ outside S, satisfying the above congruences, such that $\overline{\rho}_\ell$ is absolutely reducible. Then the semisimplification of $\overline{\rho}_\ell$ is the direct sum of two characters χ and $\omega\chi^{-1}$, where ω is the mod ℓ cyclotomic character. Moreover, E_ℓ has ordinary reduction; it follows that we can take χ to be unramified at ℓ. As $N(\overline{\rho}_\ell)$ divides N, the conductor of χ likewise divides N. Then for any p congruent to 1 modulo N, $\overline{\rho}_\ell(\mathrm{Frob}_p)$ has trace $p+1$, and so a_p is congruent to $p+1$ module ℓ for all such ℓ. If there were infinitely many such ℓ, we would then have $a_p = p+1$ violating the Weil bounds.

We have thus constructed infinitely many ℓ for which $k(\overline{\rho}_\ell) = 2$, $N(\overline{\rho}_\ell)$ divides N, and $\overline{\rho}_\ell$ is absolutely irreducible. If ℓ_i is one such ℓ, then Serre's conjecture implies there is a normalized eigenform f_i of weight 2 and level dividing N, with coefficients in an integer ring $\mathcal{O}_i$, and a prime ideal λ_i of $\mathcal{O}_i$ of residue characteristic ℓ, such that $\overline{\rho}_{f_i,\lambda_i}$ is isomorphic to $\overline{\rho}_{\ell_i}$. As the space of modular forms of weight 2 and level dividing N is finite dimensional, at least one of the above eigenforms gives rise to infinitely many of the $\overline{\rho}_{\ell_i}$. That is, there exists an eigenform f, with coefficients in $\mathcal{O}$, and infinitely many prime ideals λ_i' of $\mathcal{O}$, of residue characteristics ℓ_i', such that $\overline{\rho}_{f,\lambda_i'}$ is isomorphic to $\overline{\rho}_{\ell_i'}$ for all i. By considering the traces of Frob_p, we find that $a_p(f)$ is congruent to a_p modulo λ_i' for all i, and hence that $a_p(f) = a_p$ for all p outside S. As f is an eigenform, this is enough to conclude that f has integral coefficients. □

Theorem 4 now follows easily from the Proposition. Eichler-Shimura theory attaches to f an elliptic curve E_f over $\mathbf{Q}$, well-defined up to isogeny, such that for all p outside S, E_f has good reduction at p, and the trace of Frob_p on $T_\ell E_f$ is equal to a_p for all ℓ not equal to p. It follows that $T_\ell E_f \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$ is isomorphic to $\rho_\ell \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$ as representations of $G_{\mathbf{Q}}$.

The category of elliptic curves over $\mathbf{Q}$ is equivalent to the category of pairs $([E], L)$, where $[E]$ is an isogeny class of elliptic curves over $\mathbf{Q}$,

and L is a $G_{\mathbf{Q}}$-stable $\hat{\mathbf{Z}}$-lattice in

$$\left(\prod T_\ell E\right) \otimes_{\mathbf{Z}} \mathbf{Q}.$$

(The equivalence sends an elliptic curve E to the pair $(E, \prod T_\ell E)$.) Choosing for each ℓ a lattice in $(T_\ell E_f) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$ on which $G_{\mathbf{Q}}$ acts via ρ_ℓ thus yields the required E.

The fact that $G_{\mathbf{Q}}$ acts on $E[m]$ via ρ follows from the fact that for all ℓ^a dividing m, the reduction of ρ_ℓ modulo ℓ^a agrees with the reduction of ρ modulo ℓ^a.

Acknowledgements

We would like to thank Tong Liu for his help. The second author would like to acknowledge the support of his research by NSA grant MDA904-H98230-09-1-0070.

References

[1] N. Bruin, M. Stoll: *Deciding existence of rational points on curves: an experiment*, Experiment. Math., **17** (2008), no 2, 181–189.

[2] D. Harari, J. F. Voloch, *The Brauer-Manin obstruction for integral points on curves*, http://www.ma.utexas.edu/users/voloch/Preprints/dhvol.pdf preprint 2009.

[3] J. S. Milne: *Étale cohomology*, Princeton Mathematical Series **33**, Princeton University Press 1980.

[4] J. S. Milne: *Arithmetic duality theorems*, Second edition, BookSurge, LLC, Charleston, SC, 2006.

[5] C. Khare, J.-P. Wintenberger: *On Serre's conjecture for 2-dimensional mod p representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Ann. Math. (2) **169** (2009), no. 1, 229–253.

[6] A. Kraus: *Sur les modules Galoisiens des points de torsion des courbes elliptiques*, Sem. de Theorie des Nombres de Caen, 1990.

[7] B. Poonen, J. F. Voloch: *The Brauer-Manin obstruction for subvarieties of abelian varieties over function fields*, Annals of Math., **171** (2010) 511–532.

[8] V. Scharaschkin: *Local-global problems and the Brauer-Manin obstruction*, 1999, Ph.D. thesis, University of Michigan.

[9] J.-P. Serre: *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230.

[10] A. Silverberg: *Explicit families of elliptic curves with prescribed mod N representations*, in Modular forms and Fermat's last theorem, G. Cornell, J. Silverman, G. Stevens, eds. Springer 1997, pp. 447–461.

[11] A. N. Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics, 144, Cambridge University Press, Cambridge, 2001.

[12] M. Stoll, *Finite descent and rational points on curves*, Algebra and Number Theory **2** (2008), no 5, 595–611.

Department of Mathematics, University of Texas, Austin, TX 78712, USA
E-mail address: dhelm@math.utexas.edu
URL: http://www.ma.utexas.edu/~dhelm/

Department of Mathematics, University of Texas, Austin, TX 78712, USA
E-mail address: voloch@math.utexas.edu
URL: http://www.ma.utexas.edu/~voloch/