Remark on fundamental groups and effective Diophantine methods for hyperbolic curves

Minhyong Kim

February 21, 2013

Dedicated to the memory of Serge Lang

In a few earlier papers ([8], [9], [10]) attention was called to the striking parallel between the ideas surrounding the well-known conjecture of Birch and Swinnerton-Dyer for elliptic curves, and the mysterious *section conjecture* of Grothendieck [6] that concerns hyperbolic curves. We wish to explain here some preliminary ideas for 'effective non-abelian descent' on hyperbolic curves equipped with at least one rational point. We again follow in an obvious manner the method of descent on elliptic curves and, therefore, rely on conjectures. In fact, the main point is to substitute the section conjecture for the finiteness of the Shafarevich group. That is to say, the input of the section conjecture is of the form

section conjecture $\Rightarrow$ termination of descent

At a number of different lectures on the topic of fundamental groups and Diophantine geometry, the question was raised about the role of *surjectivity* in the section conjecture as far as Diophantine applications are concerned. This implication is intended as something of a reply.

To *start* the descent, on the other hand, requires the use of p-adic Hodge theory and the unipotent Albanese map. In this process, in general, one another conjecture is unfortunately needed. It could be, for example, the Bloch-Kato conjecture on surjectivity of the p-adic Chern class map that has been referred to in [9]. In other words, via the construction of Selmer varieties and Albanese maps, one deduces an implication

Bloch-Kato conjecture $\Rightarrow$ beginning of descent

The main caveat here arises from lack of actual knowledge of computational issues on the part of the author. To avoid misleading anyone about what is being achieved here, we have in the following section separated out the questionable portions as hypotheses [H] and [H']. That is to say, the objects that mediate this process, namely Galois cohomology groups/varieties and maps between them, seem in principle to be computable. But even to the algorithmically illiterate perspective, it is obvious that actual computation would be daunting to the point of impossibility given the technology of the present day. Nevertheless, it is perhaps not entirely devoid of value to point out one direction of investigation in effective methods, in the hope that even incompetent strategies may eventually be improved through the focussing of sharper skills obviously available in the community. Hence, the present paper.

One point of some theoretical interest concerns the comparison with 'effective Mordell conjectures' in the usual sense where upper bounds for heights are proposed. If we fix a point b on the curve and measure heights with respect to the corresponding divisor, the height of another point measures the distance from b at all places. So an upper bound for the height corresponds to a lower bound for the distance from b at all places. On the other hand, what the p-adic Hodge theory provides (in principle) is a lower bound for the p-adic distance between all pairs of points at one place. This lower bound is exactly what is required to start the descent.

Finally, we make the obvious point that the use of conjectures is probably not a serious obstacle from the computational perspective (that is, in comparison to the problem of feasibility). This is in the same spirit as the standard algorithms for computing Mordell-Weil groups of elliptic curves where the BSD conjecture is employed with just a few misgivings [3].

1 Brief review

Here we will be intentionally brief, referring the reader to [4] and [9] for a more thorough discussion.

Let $X/\mathbb{Q}$ be a proper smooth hyperbolic curve of genus g with a point $b \in X(\mathbb{Q})$ and let S be the set of primes of bad reduction for X. In the following, we shall be a bit sloppy and mostly omit separate notation for an integral model of X. Choose a prime $p \notin S$ and let $U^{et} = \pi_1^{et,\mathbb{Q}_p}(X,b)$ be the $\mathbb{Q}_p$-unipotent étale fundamental group of $\bar{X} := X \times_{\mathrm{Spec}(\mathbb{Q})} \bar{\mathbb{Q}}$ and $U_n^{et} = (U^{et})^n \backslash U^{et}$ its quotient by the n-th level of the descending central series normalized so that $(U^{et})^1 = U^{et}$. Let Γ be the Galois group of $\bar{\mathbb{Q}}$ over $\mathbb{Q}$. We defined ([9], [10]) the Selmer varieties

$$H^1_f(\Gamma, U_n^{et})$$

classifying Γ-equivariant torsors for U_n^{et} that are unramified at all places not in $\{p\} \cup S$ and crystalline at p. ($H^1_f(\Gamma_T, U_n^{et})$ in the notation of [8] and [9].) Recall the fundamental diagram ([9], end of section 2)

$$\begin{array}{ccccc} X(\mathbb{Q}) & \hookrightarrow & X(\mathbb{Q}_p) & & \\ \downarrow{\scriptstyle \kappa_n^{et,glob}} & & \downarrow{\scriptstyle \kappa_n^{et,loc}} & \searrow{\scriptstyle \kappa_n^{dr/cr}} & \\ H^1_f(\Gamma, U_n^{et}) & \xrightarrow{\mathrm{loc}_p} & H^1_f(G_p, U_n^{et}) & \xrightarrow{D} & U_n^{dr}/F^0 \end{array}$$

Here, $H^1_f(G_p, U_n^{et})$ classifies $G_p := \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$-equivariant torsors for U_n^{et} that are crystalline, while U_n^{dr}/F^0 classifies compatible pairs $T_n^{dr} \simeq T_n^{cr}$ of torsors for the De Rham and crystalline fundamental groups U_n^{dr} and U_n^{cr} equipped with Hodge filtrations and Frobenius endomorphisms compatible with the torsor structures. The maps associate to each point $x \in X(\mathbb{Q})$ the class of the torsor of paths from b to x in the appropriate category. So

$$\kappa_n^{et,glob}(x) = [\pi_1^{et,\mathbb{Q}_p}(\bar{X}; b, x)_n]$$

with Γ-action,

$$\kappa_n^{et,loc}(x) = [\pi_1^{et,\mathbb{Q}_p}(\bar{X}; b, x)_n]$$

with G_p-action, and

$$\kappa_n^{dr/cr}(x) = [\pi_1^{dr}(X \otimes \mathbb{Q}_p; b, x) \simeq \pi_1^{cr}(Y; \bar{b}, \bar{x})]$$

where Y is the reduction mod p of a smooth $\mathbb{Z}[1/S]$ model for X.

In contrast to this mass of notation, the section conjecture considers just one map

$$\hat{\kappa} : X(\mathbb{Q}) \to H^1(\Gamma, \hat{\pi}_1(\bar{X}, b))$$

that sends a point $x \in X(\mathbb{Q})$ to the class of the pro-finite torsor of paths

$$\hat{\pi}_1(\bar{X}; b, x)$$

with Γ-action. It proposes that this map should be a bijection. The injectivity is already known as a consequence of the Mordell-Weil theorem for the Jacobian J of X, while the surjectivity seems to be a very deep problem. The question mentioned in the introduction arises exactly because the injectivity appears, at first glance, to be more relevant for finiteness than the surjectivity. The idea for

using the *bijectivity* seems to have been to create a tension between the compact pro-finite topology of $H^1(\Gamma, \hat{\pi}_1(\bar{X}, b))$ and the 'discrete nature' of $X(\mathbb{Q})$. At present it is unclear how this intuition is to be realized. But, as mentioned, when the finiteness is obtained through a different approach, we wish to explain the use of the surjectivity for *finding* the full set of points.

Using the exact sequence

$$0 \to U^{n+1} \backslash U^n \to U_{n+1} \to U_n \to 0$$

for each of the fundamental groups, the global Selmer variety is fibered according to the sequence

$$0 \to H^1_f(\Gamma, (U^{et})^{n+1} \backslash (U^{et})^n) \to H^1_f(\Gamma, U^{et}_{n+1}) \to H^1_f(\Gamma, U^{et}_n)$$

which means that the kernel acts on the variety in the middle with orbit space a subset of the third object. If we denote by r_n the dimension of U_n, there is a recursive formula [11]

$$\Sigma_{i|n} i r_i = (g + \sqrt{g^2 - 1})^n + (g - \sqrt{g^2 - 1})^n$$

which implies in particular that

$$r_n \approx (g + \sqrt{g^2 - 1})^n / n.$$

The global Selmer variety has its dimension controlled by the Euler characteristic formula for the cohomology of the group $G_T = \mathrm{Gal}(\mathbb{Q}_T / \mathbb{Q})$, where $T = S \cup \{p\}$ and $\mathbb{Q}_T$ is the maximal extension of $\mathbb{Q}$ unramified outside T ([9], section 3). It reads

$$H^1(\Gamma_T, (U^{et})^{n+1} \backslash (U^{et})^n) - H^2(\Gamma_T, (U^{et})^{n+1}) \backslash (U^{et})^n) = [(U^{et})^{n+1} \backslash (U^{et})^n]^-$$

where the minus in the superscript refers to the sign for the action of complex conjugation. The dimension of this minus part can be estimated as follows. The action of complex conjugation on the étale fundamental group is compatible with the its action on the Betti realization of the motivic fundamental group [4] according to which

$$(U^B)^{n+1} \backslash (U^B)^n$$

has a pure Hodge structure of weight n. So when n is odd, we get

$$\dim[(U^{et})^{n+1} \backslash (U^{et})^n]^- = r_n / 2$$

But when $n = 2m$ is even, there is the contribution from the (m, m) component to consider, which can be complicated. This (m, m) component is a quotient of the (m, m)-part of

$$H_1(X(\mathbb{C}), \mathbb{C})^{\otimes 2m}$$

which has dimension $\binom{2m}{m} g^{2m}$. So for simplicity, we will just use the tautological estimate

$$\dim[(U^{et})^{n+1} \backslash (U^{et})^n]^- \leq r_n$$

for n even.

In [9], section 3, we analyzed already the use of the corresponding Shafarevich groups

$$Sha^2((U^{et})^{n+1} \backslash (U^{et})^n)) := Ker[H^2(\Gamma_T, (U^{et})^{n+1} \backslash (U^{et})^n) \to \oplus_{v \in T} H^2(\Gamma_v, (U^{et})^{n+1} \backslash (U^{et})^n)]$$

which is dual to

$$Sha^1(((U^{et})^{n+1} \backslash (U^{et})^n)^*(1)) := Ker[H^1(\Gamma_T, ((U^{et})^{n+1} \backslash (U^{et})^n)^*(1)) \to \oplus_{v \in T} H^1(\Gamma_v, ((U^{et})^{n+1} \backslash (U^{et})^n)^*(1))]$$

There is a Chern class map [1]

$$ch_{n,1} : K^{(1)}_{2-n-1}(X^n) \otimes \mathbb{Q}_p \to H^1(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), H^n(\bar{X}^n, \mathbb{Q}_p(1)))$$

for $n \neq 1$ whose image lies in a 'geometric' subspace

$$H^1_g(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), H^n(\bar{X}^n, \mathbb{Q}_p(1)))$$

that contains

$$Sha^1(H^n(\bar{X}^n, \mathbb{Q}_p(1)))$$

In fact,

$$Sha^1([(U^{et})^{n+1}\backslash(U^{et})^n)]^*(1))$$

is a subspace of $Sha^1(H^n(\bar{X}^n, \mathbb{Q}_p(1)))$ because the representation $(U^{et})^{n+1}\backslash(U^{et})^n$ is a direct summand of $H^{et}_1(\bar{X}, \mathbb{Q}_p)^{\otimes n}$ which, in turn, is a direct summand of $(H^n(\bar{X}^n, \mathbb{Q}_p))^*$. But Bloch and Kato conjecture that

$$ch_{n,1} : K^{(1)}_{2-n-1}(X^n) \otimes \mathbb{Q}_p \rightarrow H^1_g(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), H^n(\bar{X}^n, \mathbb{Q}_p(1)))$$

is an isomorphism. Thus, when $n \geq 2$, we get

$$Sha^1([(U^{et})^{n+1}\backslash(U^{et})^n)]^*(1)) = 0$$

We recall the explicit bound for the local H^2 ([9], section 3). For $v \neq p$, we have

$$\dim H^2(G_v, (U^{et})^{n+1}\backslash(U^{et})^n) \leq ng^n + \frac{n(n-1)}{2}(2g-2)^2 g^{n-2}$$

while

$$\dim H^2(G_p, (U^{et})^{n+1}\backslash(U^{et})^n) \leq ng^n$$

Finally, as regards the contribution of the Hodge filtration, we saw in loc. cit. that

$$F^0((U^{dr})^{n+1}\backslash(U^{dr})^{n+1}) \leq g^n$$

so that

$$\dim(U^{dr})^{n+1}\backslash(U^{dr})^{n+1}/F^0 \geq r_n - g^n \approx (g + \sqrt{g^2-1})^n/n - g^n$$

2 Beginning the descent

Since it costs very little extra work to define, we will in fact consider the refined Selmer variety

$$H^1_{f,0}(\Gamma, U^{et}_n) \subset H^1_f(\Gamma, U^{et}_n)$$

consisting of classes whose images in

$$H^1_f(\Gamma, U^{et}_2)$$

go to zero under all localization maps

$$H^1_f(\Gamma, U^{et}_2) \stackrel{\mathrm{loc}_v}{\rightarrow} H^1(G_v, U^{et}_2)$$

for $v \neq p$. As explained in [10], the image of $X(\mathbb{Q})$ under $\kappa^{et,glob}_n$ lies in $H^1_{f,0}(\Gamma, U^{et}_n)$. From the estimates of the previous section, it is obvious that

assuming the Bloch-Kato conjecture, there is an effectively computable t such that

$$dim H^1_{f,0}(\Gamma, U^{et}_n) < dim U^{dr}_n/F^0$$

for $n \geq t$.

Of course the computation starts out with an estimate for $\dim H^1_{f,0}(\Gamma, U^{et}_2)$ which according to the usual BSD is the same as the Mordell-Weil rank of J. After that the dimension of $\dim H^1_{f,0}(\Gamma, U^{et}_n)$

grows as a function of n with an explicit upper bound while the dimension of U_n^{dr}/F^0 grows with an explicit (and eventually bigger) lower bound. Written out, the estimate for growth looks like

$$\dim H^1_{f,0}(\Gamma, U^{et}_{2n+1}) \leq \dim H^1_{f,0}(\Gamma, U^{et}_{2n}) + r_{2n}/2 + |S|[(2n)g^{2n} + \frac{(2n)(2n-1)}{2}(2g-2)^2 g^{2n-2}] + (2n)g^{2n}$$

and

$$\dim H^1_{f,0}(\Gamma, U^{et}_{2n+2}) \leq \dim H^1_{f,0}(\Gamma, U^{et}_{2n+1}) + r_{2n+1} + |S|[(2n+1)g^{2n+1} + \frac{(2n+1)(2n)}{2}(2g-2)^2 g^{2n-1}] + (2n+1)g^{2n+1}$$

while

$$\dim U_{n+1} \geq \dim U_n + r_n - g^n$$

We eventually get an inequality in the right direction because of the asymptotic behavior of r_n. In this regard, note that $g + \sqrt{g^2-1} > g$ for $g \geq 2$.

As a consequence of the discrepancy in dimension, the image of

$$D \circ \mathrm{loc}_p : H^1_{f,0}(\Gamma, U_t^{et}) \rightarrow U_t^{dr}/F^0$$

is *not* Zariski dense. In contrast to difficult sets like $X(\mathbb{Q})$, the classifying spaces for torsors and the maps between them are algebro-geometric objects which can be computed in principle. This should work in the manner of computations with the usual method of Chabauty as appears, for example, in [7] (cf. the discussion of θ in the introduction). In case this is not convincing, we will adopt it as an additional hypothesis:

[H]: The map

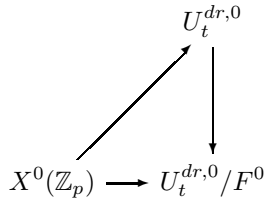
$$D \circ \mathrm{loc}_p : H^1_{f,0}(\Gamma, U_t^{et}) \rightarrow U_t^{dr}/F^0$$

can be computed.

The end result of this is that assuming B-K and [H], we can find an algebraic function α on U_t^{dr}/F^0, that vanishes on the image of $H^1_{f,0}(\Gamma, U_t^{et})$. Now, when we restrict α to $X(\mathbb{Q}_p)$ it becomes a linear combination of p-adic iterated integrals. To elaborate on this point a little more, recall ([9], section 1) the description of the coordinate ring of the De Rham fundamental group $U^{dr,0}$ for an affine curve X^0 obtained by deleting some rational divisor from X. In this case, when we choose a collection $a_1, a_2, \ldots, a_k$ of algebraic differential forms on X^0 inducing a basis of $H^1_{dr}(X^0)$, the coordinate ring of $U^{dr,0}$ has the form

$$\mathbb{Q}_p < a_w >,$$

the $\mathbb{Q}_p$ vector space generated by symbols a_w, one for each finite sequence w of numbers from $\{1, 2, \ldots, k\}$. Furthermore, on $X^0(\mathbb{Z}_p)$, there is a lifting (depending on the previous choice of basis)



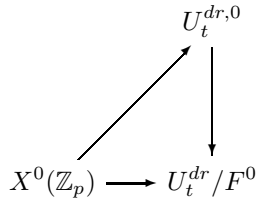
such that the restriction of a_w for $w = (i_1, i_2, \ldots, i_l)$ to $X^0(\mathbb{Z}_p)$ has the form

$$a_w(z) = \int_b^z a_{i_1} a_{i_2} \cdots a_{i_l}$$

Also, there is a functorial map

$$U_t^{dr,0} \rightarrow U_t^{dr}$$

compatible with the Hodge filtration so that the function α on U_t^{dr}/F^0 can be lifted to $U_t^{dr,0}$. That is to say, one can construct a diagram



enabling us to compute the restriction of α to $X^0(\mathbb{Z}_p)$ in terms of the a_w. The idea would be to carry this process out for two separate affine X^0 so as to cover $X(\mathbb{Z}_p)$ and then to express α in terms of iterated integrals on each affine open set. Of course, the problem of explicitly computing the local liftings is also a daunting task, although possible in theory. The author makes no pretense of knowing, as yet, how to reduce this to a tractable process. Perhaps it is safer to state it also explicitly as a hypothesis:

[H']: The map

$$U_t^{dr,0} \longrightarrow U_t^{dr}/F^0$$

can be computed.

Choose a representative $y \in X(\mathbb{Q}_p)$ for each point in $Y(\mathbb{F}_p)$ ($= X \bmod p$) and a coordinate z_y centered at y. We must then approximate the zeros of α on $X(\mathbb{Q}_p)$ by expressing it as a power series in the z_y. This needs to be carried out to a sufficiently high degree of accuracy so that we can find an M and a finite collection $y_i \in X(\mathbb{Q}_p)$ for which

$$]y_i[_M := \{x \in X(\mathbb{Q}_p) | z_{y_i}(x) \leq p^{-M}\}$$

contains at most one zero of α. That is to say, we need to separate the zeros of α modulo p^M. Note that even at this point, since all expressions will be approximate, there would be no way to determine which of the y_i relate to actual points of $X(\mathbb{Q})$, even though an upper bound for the *number* of points may be available, as was emphasized by Coleman [2]. In fact, the process of separating the points using small disks already seems to occur, at least implicitly, in the method of Coleman-Chabauty. In the next section we will see how to combine that separation with the section conjecture.

We summarize the preceding passages as follows:

Observation 1 *Assuming the Bloch-Kato conjecture and the hypotheses [H] and [H'], there is an effectively computable M such that the map*

$$X(\mathbb{Q}) \hookrightarrow X(\mathbb{Q}_p) \rightarrow X(\mathbb{Z}/p^M)$$

is injective.

In our view, this statement is one rather essential justification for studying the Selmer varieties and unipotent Albanese maps. That is, Faltings' theorem as it stands does not seem to give, even in principle, a way of getting at this sort of effectivity. To belabor the obvious, the point is that the map

$$X(\mathbb{Q}) \rightarrow X(\mathbb{Q}_p)$$

is not a priori (i.e., before finding $X(\mathbb{Q})$) computable even in principle, while

$$H^1_{f,0}(\Gamma, U_t^{et}) \rightarrow U_t^{dr}/F^0$$

is.

When we embed $X(\mathbb{Q})$ inside $J(\mathbb{Q})$ using the base-point b, we see then that we have an injection

$$X(\mathbb{Q}) \hookrightarrow J(\mathbb{Z}/p^M)$$

But the kernel of the reduction map

$$J(\mathbb{Q}) \to J(\mathbb{Z}/p^M)$$

is of finite index, and hence, contains $NJ(\mathbb{Q})$ for some N. So finally, we arrive at an effectively computable N such that

$$X(\mathbb{Q}) \to J(\mathbb{Q}) \to J(\mathbb{Q})/NJ(\mathbb{Q})$$

is injective. Let T_0 be S together with the set of primes dividing N and Γ_{T_0} the fundamental group of $\mathrm{Spec}(\mathbb{Z}[1/T_0])$ with base-point given by $\mathbb{Z}[1/T_0] \hookrightarrow \mathbb{Q} \hookrightarrow \bar{\mathbb{Q}}$. Then we get an injection

$$X(\mathbb{Q}) \hookrightarrow H^1(\Gamma_{T_0}, J[N])$$

allowing us to begin descent.

3 Non-abelian descent and its termination

Once we have the final conclusion of the previous section, we can dispense entirely with the unipotent machinery and start to deal with the pro-finite formalism. There are many ways to construct a co-final system for

$$\Delta := \hat{\pi}_1(\bar{X}, b)$$

of which we will use one described in a letter from Deligne to Thakur [5]. Let $K_n \subset \Delta$ be the intersection of all open subgroups of index $\leq n$. It is a characteristic subgroup, and hence, we can form the quotient $\Delta(n) := \Delta/K_n$. The order of this quotient has all prime divisors $\leq n$. Let Γ_n denote the fundamental group of $\mathrm{Spec}(\mathbb{Z}[1/n!])$. We also denote by $\pi(n)$ the quotient of $\hat{\pi}_1(X, b)$ by K_n, a group that fits into the exact sequence

$$0 \to \Delta(n) \to \pi(n) \to \Gamma \to 0.$$

For n larger than any prime in S, there is a pull-back diagram ([12], proof of theorem 2.8)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Delta(n) & \longrightarrow & \pi(n) & \longrightarrow & \Gamma & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \Delta(n) & \longrightarrow & \hat{\pi}_1(\mathcal{X}_n)/K_n & \longrightarrow & \Gamma_n & \longrightarrow & 0 \end{array}$$

where $\mathcal{X}_n$ is a proper smooth model for X over $\mathrm{Spec}(\mathbb{Z}[1/n!])$. Therefore, we see that any point $x \in X(\mathbb{Q})$ defines a class in

$$H^1(\Gamma_n, \Delta(n))$$

and that we have a commutative diagram

$$\begin{array}{ccc} X(\mathbb{Q}) & \xrightarrow{\hat{\kappa}} & H^1(\Gamma, \Delta) \\ \downarrow & & \downarrow \\ H^1(\Gamma_n, \Delta(n)) & \hookrightarrow & H^1(\Gamma, \Delta(n)) \end{array} \tag{1}$$

There is a sequence of subsets containing $X(\mathbb{Q})$,

$$H^1(\Gamma,\Delta)_i \subset H^1(\Gamma,\Delta)$$

consisting of those classes whose projection to $H^1(\Gamma,\Delta(i))$ lie in the image of

$$H^1(\Gamma_i,\Delta(i))\hookrightarrow H^1(\Gamma,\Delta(i))$$

Let n_0 be larger than the primes in T_0. Then we have diagrams

$$\begin{array}{ccc} H^1(\Gamma,\Delta)_i & \hookrightarrow & H^1(\Gamma,\Delta) \\ \downarrow & & \downarrow \\ H^1(\Gamma_i,\Delta(i)) & \hookrightarrow & H^1(\Gamma,\Delta(i)) \\ \downarrow & & \\ H^1(\Gamma_{T_0},J[N]) & \hookrightarrow & H^1(\Gamma_i,J[N]) \end{array} \tag{2}$$

for $i \geq n_0$. Using this, we can define a decreasing sequence of subsets

$$H^1(\Gamma_{T_0},J[N])_n \subset H^1(\Gamma_{T_0},J[N])$$

for $n \geq n_0$ consisting of those classes whose images in $H^1(\Gamma_i,J[N])$ lift to $H^1(\Gamma_i,\Delta(i))$ for all $n_0 \leq i \leq n$. For $n \geq n_0$, we also have a commutative diagram

$$\begin{array}{ccc} X(\mathbb{Q}) & \hookrightarrow & H^1(\Gamma_n,\Delta(n)) \\ \downarrow & & \downarrow \\ H^1(\Gamma_{T_0},J[N]) & \hookrightarrow & H^1(\Gamma_n,J[N]) \end{array} \tag{3}$$

Meanwhile, there is an increasing sequence

$$X(\mathbb{Q})_n \subset X(\mathbb{Q}) \subset H^1(\Gamma_{T_0},J[N])$$

consisting of the points with height (in some projective embedding) $\leq n$. We visualize the situation using the sort of diagram familiar from the arithmetic theory of elliptic curves:

$$\cdots X(\mathbb{Q})_n \subset X(\mathbb{Q})_{n+1} \subset \cdots \subset H^1(\Gamma_{T_0},J[N])_{m+1} \subset H^1(\Gamma_{T_0},J[N])_m \subset \cdots \subset H^1(\Gamma_{T_0},J[N])$$

Observation 2 *The section conjecture implies that*

$$X(\mathbb{Q})_n = H^1(\Gamma_{T_0},J[N])_m$$

for n,m sufficiently large. At this point, $X(\mathbb{Q}) = X(\mathbb{Q})_n$.

That is to say, we know when to stop searching. The simple proof is written out just to make sure the author is not confused.

Proof. Assume the section conjecture. Then by diagrams (1) and (2), we have

$$H^1(\Gamma,\Delta)_i = H^1(\Gamma,\Delta)$$

for all i and we actually have maps

$$H^1(\Gamma, \Delta) \to H^1(\Gamma_i, \Delta(i))$$

for each i. Furthermore since $H^1(\Gamma, \Delta)$ is finite (which follows either from Faltings theorem or the reproof assuming Bloch-Kato from the previous section) we have

$$H^1(\Gamma, \Delta) \simeq H^1(\Gamma_i, \Delta(i))$$

for i sufficiently large. So if $c \in H^1(\Gamma_{T_0}, J[N])$ is not in $X(\mathbb{Q})$, then $c \notin H^1(\Gamma_{T_0}, J[N])_m$ for some m. Thus, eventually, $X(\mathbb{Q}) = H^1(\Gamma_{T_0}, J[N])_m$. Of course eventually $X(\mathbb{Q})_n = X(\mathbb{Q})$. Now suppose

$$X(\mathbb{Q})_n = H^1(\Gamma_{T_0}, J[N])_m$$

at any point. Then classes not in $H^1(\Gamma_{T_0}, J[N])_m$ cannot lift to $H^1(\Gamma, \Delta)_m$. And hence, they are not in $X(\mathbb{Q})$. That is to say, $X(\mathbb{Q})_n = X(\mathbb{Q})$. $\square$

All the cohomology sets occurring in the argument are finite and thereby have the nature of being computable through explicit Galois theory. As mentioned in the introduction, the actual implementation of such an algorithm is obviously an entirely different matter.

Acknowledgements:
-The author was supported in part by a grant from the National Science Foundation and a visiting professorship at RIMS.
-He is grateful to Kazuya Kato, Shinichi Mochizuki, and Akio Tamagawa for a continuing stream of discussions on topics related to this paper, and for their generous hospitality during the Fall of 2006.

References

[1] Bloch, Spencer; Kato, Kazuya L-functions and Tamagawa numbers of motives. *The Grothendieck Festschrift, Vol. 1*, 333–400, Prog. Math. 86, Birkhäuser, Boston, MA 1990.

[2] Coleman, Robert F. Effective Chabauty. Duke Math. J. 52 (1985), no. 3, 765–770.

[3] Cremona, John *Algortihms for elliptic curves.* Online edition available at http://www.maths.nott.ac.uk/personal/jec/book/fulltext/index.html

[4] Deligne, Pierre Le groupe fondamental de la droite projective moins trois points. Galois groups over $\mathbb{Q}$ (Berkeley, CA, 1987), 79–297, Math. Sci. Res. Inst. Publ., 16, Springer, New York, 1989.

[5] Deligne, Pierre Letter to Dinesh Thakur. March 7, 2005.

[6] Grothendieck, Alexandre Brief an G. Faltings, *Geometric Galois Actions, 1*,49–58, London Math. Soc. Lecture Note Ser., 242, Cambridge University Press, Cambridge, 1997.

[7] Flynn, Victor A Flexible Method for Applying Chabauty's Theorem. Compositio Math. 105 (1997), 7994.

[8] Kim, Minhyong The motivic fundamental group of $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel. Invent. Math. 161 (2005), no. 3, 629–656.

[9] Kim, Minhyong The unipotent Albanese map and Selmer varieties for curves. math.NT/0510441 (submitted).

[10] Kim, Minhyong; Tamagawa, Akio The l-component of the unipotent Albanese map. Arxiv preprint math.NT/0611384.

[11] Labute, John P. On the descending central series of groups with a single defining relation. J. Algebra 14 1970 16–23.

[12] Wildeshaus, Jörg Realizations of polylogarithms. Lecture Notes in Mathematics, 1650. Springer-Verlag, Berlin, 1997.

DEPARTMENT OF MATHEMATICS, PURDUE UNIVERSITY, WEST LAFAYETTE, INDIANA 47907 and DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ARIZONA, TUCSON, AZ 85721, U.S.A.

EMAIL: kimm@math.purdue.edu