CONTRIBUTED PROBLEMS

RATIONAL POINTS AND GALOIS REPRESENTATIONS, MAY 2021

This document is a compilation of problems and questions recorded at the workshop *Rational Points and Galois Representations*, hosted by the University of Pittsburgh. The first four items are summaries of advance contributions to the workshop's problem session, which occurred on May 12, 2021. The organizers thank the problem contributors as well as the session moderator, David Zureick-Brown.

Contents.

A CHABAUTY–COLEMAN SOLVER FOR CURVES OVER NUMBER FIELDS

JENNIFER BALAKRISHNAN

For a number of applications (in particular, computing K-rational points on curves over number fields K [Col85a]), it would be very useful to have an implementation of Coleman integration [Col85b] for curves over extensions of the p-adics. In [BT20], Tuitman and I gave an algorithm and `Magma` implementation [BT] of Coleman integration for curves over $\mathbf{Q}_p$. It would be great to extend this to handle curves defined over unramified extensions of $\mathbf{Q}_p$. (See the work of Best [Bes21] for the case of superelliptic curves over unramified extensions of $\mathbf{Q}_p$, combined with algorithmic improvements along the lines of work of Harvey [Har07].)

With this in hand, one could then further implement a Chabauty–Coleman solver for curves over number fields that would take as input a genus g curve X defined over a number field K with Mordell–Weil rank r less than g, a prime $\mathfrak{p}$ of good reduction, and r generators of the Mordell–Weil group modulo torsion and output the finite Chabauty–Coleman set $X(K_{\mathfrak{p}})_1$, which contains the set $X(K)$.

References

[Bes21] A. J. Best. Square root time Coleman integration on superelliptic curves. In *Arithmetic Geometry, Number Theory, and Computation*. Springer, 2021. https://alexjbest.github.io/papers/coleman-superelliptic.pdf

[BT] J. S. Balakrishnan and J. Tuitman. Magma code. https://github.com/jtuitman/Coleman.

[BT20] J. S. Balakrishnan and J. Tuitman. Explicit Coleman integration for curves. *Math. Comp.*, 89(326):2965–2984, 2020.

[Col85a] R. F. Coleman. Effective Chabauty. *Duke Math. J.*, 52(3):765–770, 1985.

[Col85b] R. F. Coleman. Torsion points on curves and p-adic abelian integrals. *Ann. of Math. (2)*, 121(1):111–168, 1985.

[Har07] D. Harvey. Kedlaya's algorithm in larger characteristic. *Int Math Res Notices*, 2007(rnm095):rnm095–29, 2007.

E-mail address: jbala@bu.edu

GALOIS ACTION ON SLIGHTLY NONABELIAN FUNDAMENTAL GROUPS

JORDAN S. ELLENBERG

Much of what we know how to say about a variety X over a field K has to do with the action of $\mathrm{Gal}(K)$ on the étale cohomology of $X_{\bar{K}}$. More precisely, this Galois action, if $\mathrm{Gal}(K)$ is "big enough," tells us a lot about the arithmetic of the Jacobian $J(X)$, from which in turn we can learn a lot about X itself. A huge amount of energy has gone into understanding properties of this Galois representation and explicit methods for computing it for varieties we may encounter.

The first étale cohomology group – or, more precisely, its dual – can be thought of as the maximal abelian quotient of the *étale fundamental group* of $X_{\bar{K}}$, a profinite group denoted $\pi_1(X_{\bar{K}})$ which also carries an action of $\mathrm{Gal}(K)$. This action often carries much more information than its abelianization does. For example, if X is a curve, the étale cohomology only "knows about" the Jacobian of X; in particular, two curves with isogenous Jacobians will have the same Galois representations (at least after tensoring coefficients with $\mathbb{Q}$.) By contrast, the "anabelian philosophy" suggests that knowledge of the profinite group $\pi_1(X_{\bar{K}})$ together with the action of $\mathrm{Gal}(K)$, when K is a number field, should encode not only the isomorphism class of X but also the set of rational points $X(K)$. (This last part is the *section conjecture* of Grothendieck.) Even very small quotients of the fundamental group encode important geometric invariants of a curve such as its *Ceresa class* – see e.g. "Group-theoretic Johnson classes and a non-hyperelliptic curve with torsion Ceresa class" by Bisogno, Li, Litt and Srinivasan for a recent view on this story.

However, a computational apparatus comparable to what we have for étale cohomology is completely lacking. Whether this is because there's a fundamental difficulty or because people haven't tried that hard is not clear to me. Of course, the étale fundamental group is a very big place and trying to understand the *entire* Galois action on it, computationally or otherwise, is probably too big a cookie to chew. But it would even be interesting to understand how Galois acts on natural quotients of the fundamental group. For instance, the action of Galois on the quotient of π_1 by the third term of its lower central series is what encodes the Ceresa class. To what extent is this action computable in practice? Alternately, one can consider very special cases, like that where U is an genus-1 curve X with two rational points removed. In this case, π_1 is isomorphic to a profinite free group on three generators. The data of U is essentially equivalent to the data of an elliptic curve E (the Jacobian of X) together with a rational point P on that elliptic curve (the difference of the two punctures.) What is the relationship between the Galois action on the fundamental group and the pair (E, P)?

For all these questions, we have a pretty good picture of what happens when K is $\mathbb{C}((t))$, in which case we are talking about a situation that can be well-modelled by topology. (See my paper with Daniel Corey and Wanlin Li for a description of this.) The case where K is a number field is of course a lot richer and harder. But even the case where K is finite, so we're just asking about Frobenius, seems to me to have a lot of arithmetic interest!

Date: 12 May 2021.

Diophantine Geometry and Reciprocity Laws

Minhyong Kim

Question

Given a variety X over a number field F, are there nice equations defining $X(F)$ inside $X(\mathbb{A}_F)$?

Examples

1. (Manin) We have

$$X(F) \subset X(\mathbb{A}_F)^{Br}$$

Here, given any element $b \in Br(X) = H^2(X, \mathbb{G}_m)$, get a function

$$f_b : X(\mathbb{A}_F) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

$$(x_v) \mapsto (x_v^*(b)) \in \bigoplus H^2(F_v, \mathbb{G}_m) \simeq \bigoplus \mathbb{Q}/\mathbb{Z} \xrightarrow{\Sigma} \mathbb{Q}/\mathbb{Z}.$$

2. Classical reciprocity for $X = \mathbb{G}_m$:

$$\mathbb{G}_m(F) \subset Ker[\mathbb{G}_m(\mathbb{A}_F) \xrightarrow{rec} G_F^{ab}].$$

In particular, given a function ϕ on G_F^{ab} that vanishes at the origin, e.g., a $p-$adic character, get

$$\mathbb{G}_m(F) \subset Z(\phi \circ rec).$$

For a concrete example, take $\phi = \log \chi_{cyc}^p$.

3. For a smooth variety X satisfying some cohomological conditions,

$$\begin{array}{ccccccccc}
\cdots & X(\mathbb{A}_F)^4 & \subset & X(\mathbb{A}_F)^3 & \subset & X(\mathbb{A}_F)^2 & \subset & X(\mathbb{A}_F) \\
 & || & & || & & || & & || \\
\cdots & rec_3^{-1}(0) & \subset & rec_2^{-1}(0) & \subset & rec_1^{-1}(0) & \subset & X(F) \\
 & \downarrow{\scriptstyle rec_4} & & \downarrow{\scriptstyle rec_3} & & \downarrow{\scriptstyle rec_2} & & \downarrow{\scriptstyle rec_1} \\
\cdots & \mathfrak{R}_4 & & \mathfrak{R}_3 & & \mathfrak{R}_2 & & \mathfrak{R}_1
\end{array}$$

where

$$\mathfrak{R}_n := H^1(G_F, Z_n^\vee(1))^\vee$$

and Z_n are the graded subquotients of the lower central series of the $\mathbb{Q}_p$-unipotent fundamental group of X.

Fact:

$$X(F) \subset \cap_{n=1}^{\infty} Ker(rec_n).$$

Conjecture: When $F = \mathbb{Q}$,

$$X(\mathbb{Q}) = Pr_p(\cap_{n=1}^{\infty} Ker(rec_n)) \subset X(\mathbb{Q}_p)$$

Challenge:

(1) Make these explicit;

(2) Find a general formulation.

A question about quadratic points on $X_0(N)$

Barry Mazur

A general theorem of Faltings has as a particular consequence that, fixing any positive integer N and ranging over all non-CM elliptic curves defined over $\mathbb{Q}$ there are only finitely many such curves that have a **sporadic** cyclic N-isogeny rational over some quadratic field. "Sporadic" means that the N-isogeny is *not* a member of a family of such "quadratic" cyclic N-isogenies that can be parametrized either by

- rational points on a curve of genus 0 or 1, the parametrization given by a degree two correspondence between the curve and $X_0(N)$;

- or in the case where $X_0(N)$ is of genus two, by a degree two correspondence between an abelian surface and $X_0(N)$.

It is natural to ask

- whether there are only finitely many sporadic cyclic isogenies; equivalently, whether there are none at all when $N \gg 0$.
- related questions about specific examples.

A family of examples with $r > g$ and some questions

Kirti Joshi

May 12, 2021

§ 0.1 In [Joshi and Tzermias, 1999] we showed proved the following.

Theorem 0.1.1. *Let $p \geq 5$ be a prime. Let $a_0, a_1, \ldots, a_{p-1} \in \mathbb{Z}$ be integers and let $d \neq 0$ be an integer. Suppose that*

(1) *for $1 \leq i \neq j \leq p-1$, one has $a_i \neq a_j \bmod p$ (i.e. the p residue classes $a_i \bmod p$ are pairwise distinct),*

(2) *$f(x) = (x-a_0)(x-a_1)\cdots(x-a_{p-1}) + p^2d^2 \in \mathbb{Q}[x]$ is an irreducible polynomial, and*

(3) *Let $X/\mathbb{Q}$ be the hyperelliptic curve*

$$X : y^2 = f(x) = (x-a_0)(x-a_1)\cdots(x-a_{p-1}) + p^2d^2.$$

Then $X/\mathbb{Q}$ has $2g$ rational points $(a_i, \pm pd) \in X(\mathbb{Q})$ which generate a subgroup of rank $r \geq 2g$ in the Mordell-Weil group $J(\mathbb{Q})$ of the Jacobian J of X.

§ 0.2 Note X has genus $g = p-1/2$ and has good reduction modulo $p = 2g+1$. The classical Coleman-Chabauty Theorem requires $p \geq 2g+1$, so in the above examples $p = 2g+1$ is at the smallest allowed prime in the classical Coleman-Chabauty method.

§ 0.3 The lower bound we prove is not optimal. Homero R. GALLEGOS–RUIZ showed that for

$$y^2 = (x+19)(x+20)(x+21)(x+22)(x+23) + 5^2 \cdot 4^2,$$

one has $r = 5 \geq 4$.

§ 0.4 Evidently the family of examples above lie beyond $r \leq g$ case of Coleman-Chabauty-Kim method. So my questions: (perhaps ignorant questions, perhaps difficult)

(1) Can one make Coleman-Chabauty-Kim explicit in these examples?

(2) Can one understand bounds for $\#X(\mathbb{Q})$ (explicit bounds obtained by Betts, ... by Coleman-Chabauty-Kim method) as a function of $(a_0, a_1, \cdots, a_{p-1}, d, p)$?

(3) For these curves, write $X(\mathbb{Q}_p) \supseteq X(\mathbb{Q}_p)_1 \supseteq X(\mathbb{Q}_p)_2 \supseteq \cdots \supseteq X(\mathbb{Q}_p)_n \cdots \supset X(\mathbb{Q})$ for the loci provided by Coleman-Chabauty-Kim. One expects $X(\mathbb{Q}_p)_n = X(\mathbb{Q})$ for some $n < \infty$. Suppose this does happen for every X considered here. Can one understand the variation of the minimal such n as a function of $(a_0, a_1, \cdots, a_{p-1}, d, p)$ or as a function of $(a_0, a_1, \cdots, a_{p-1}, d)$ with p fixed?

(4) Is it true that for p fixed (so J has dimension $2g = p-1$) one has

$$\sup(r((a_0, a_1, \cdots, a_{p-1}, d))) < \infty?$$

(5) Perhaps these question are naive, or difficult and perhaps there is no simple answer to any of these questions. But I am unclear on what is known or what to expect here.

References

Kirti Joshi and Pavlos Tzermias. On the Coleman-Chabauty bound. *C. R. Acad. Sci. Paris Sér. I Math.*, 329(6):459–463, 1999. URL https://doi.org/10.1016/S0764-4442(00)80041-5.

MATH. DEPARTMENT, UNIVERSITY OF ARIZONA, 617 N SANTA RITA, TUCSON 85721-0089, USA.
Email: kirti@math.arizona.edu

Restriction of Scalars Chabauty and Solving Systems of Simultaneous p-adic Power Series

Nicholas Triantafillou

June 14, 2021

1 Restriction of Scalars Chabauty and Solving Systems of Simultaneous p-adic Power Series

1.1 Summary of RoS Chabauty

When X/K is a curve over a number field of degree d, it is possible to refine Chabauty's method by replacing X and its Jacobian J with their restrictions of scalars $\text{Res}_{K/\mathbb{Q}}X$ and $\text{Res}_{K/\mathbb{Q}}J$. We will assume that we have fixed a base-point $P_0 \in (\text{Res}_{K/\mathbb{Q}}X)(\mathbb{Q}) = X(K)$ and that $j : \text{Res}_{K/\mathbb{Q}}X \hookrightarrow \text{Res}_{K/\mathbb{Q}}J$ is the Abel-Jacobi map with respect to this embedding. The strategy is as follows:

1. Compute generators for the Mordell-Weil group $(\text{Res}_{K/\mathbb{Q}}J)(\mathbb{Q}) = J(K)$.
2. Compute (at least) d annihilating differentials $\omega_1, \dots, \omega_d \in H^0((\text{Res}_{K/\mathbb{Q}}J)_{\mathbb{Q}_p}, \Omega^1)$.
3. In each p-adic polydisc of $(\text{Res}_{K/\mathbb{Q}}X)(\mathbb{Q}_p)$, choose a point P and local parameters $t_1, \dots, t_d$ and compute the integrals $F_i(t_1, \dots, t_d) \coloneqq \int_{P_0}^{P+(t_1,\dots,t_d)} j^*\omega_i$.
4. On each p-adic polydisc, compute the common zeros of the F_i, hopefully as a finite list of isolated points, but possibly as a finite list of irreducible analytic subvarieties.

This restriction of scalars variant will often produce a finite list of points when $\text{rank}\, J(K) \leq d(\text{genus}(X)-1)$. However, the restriction of scalars Chabauty's method can produce an infinite set even if this inequality is satisfied. For a more detailed description of the method, including reasons why it may not always produce a finite set, see [Sik13] and [Tri19].

1.2 Project: Computing simultaneous zeros of several (separable) multivariate p-adic power series

The main additional input needed to run restriction of scalars Chabauty is a practical implementation to compute the common zero set of several multivariable p-adic power series. As such, we propose the following project.

Project 1a: Develop a practical implementation of an algorithm with the following specifications.

Given: A set of d power series $F_1, \ldots, F_d \in \mathbb{Q}_p[[t_1, \ldots t_d]]$ which converge on the p-adic polydisc $(p\mathbb{Z}_p)^d$.
Returns: Either:

1. The simultaneous zeros in $(p\mathbb{Z}_p)^d$ of $F_1, \ldots, F_d$ as a finite list of points $P_1, \ldots, P_r \in (p\mathbb{Z}_p)^d$, with enough p-adic precision to determine the points P_j completely via Hensel-lifting, or

2. Information why the algorithm failed. For instance, it could report if the F_i are not specified to large enough p-adic or t_i-adic precision, or if the common vanishing locus might have a positive-dimensional component.

This project is asking for an implementation of a multivariate version of Hensel's lemma. See Appendix A of [BBBM] for a discussion and implementation of the 2-variable case, based on [Con].

Project 1b: Complete a $K_\mathfrak{p}$-adic version of the project under the additional assumption that the power series $F_1, \ldots, F_d \in K_\mathfrak{p}[[t_1, \ldots t_d]]$ are separable, i.e. that there exist $F_{i,k} \in K_\mathfrak{p}[[t_k]]$ satisfying $F_i = \sum_{k=1}^{d} F_{i,k}$.

Project 2: Building on the other projects, develop a full implementation of Restriction of Scalars Chabauty's method to compute K-rational points on curves over number fields.

References

[BBBM] Balakrishnan, J. S., Besser, A., Bianchi, F., and Müller, J.S. "Explicit quadratic Chabauty over number fields," arxiv:1910.04653, to appear, *Israel Journal of Mathematics*.

[Con] Conrad, K. "A multivariable Hensel's lemma," `https://kconrad.math.uconn.edu/blurbs/gradnumthy/multivarhensel.pdf`

[Sik13] Siksek, S. "Explicit Chabauty over number fields." *Algebra & Number Theory* 7.4 (2013): 765-793.

[Tri19] Triantafillou, N. "Restriction of Scalars Chabauty and the S-unit equation." arXiv:2006.10590, 2020.

ADDITIONAL QUESTIONS AND COMMENTS

COMPILED BY JACKSON S. MORROW

ABSTRACT. This note contains some questions and comments from participants during the workshop *Rational Points and Galois Representations*, May 2021.

1. Questions related to Jennifer Balakrishnan's presentation in the Problem Session

Nils Bruin. As part of Chabauty–Coleman solver infrastructure, also pay attention to the case of curves mapping into Weil restrictions of elliptic curves. These cases happen surprisingly often in practical cases and information on the Mordell–Weil group is much more accessible on such abelian varieties. Support for these is already available in Magma, so efforts in this direction should probably build on that and/or port over the functionality to another platform.

Kevin Buzzard. Produce a certificate for the computation of the points on the curve of the Chabauty–Coleman solver.

2. Other questions

Jordan Ellenberg. Suppose you have two elliptic curves $E_1, E_2/\mathbb{Q}$ of conductors N_1 and N_2, and write N for $\gcd(N_1, N_2)$. Then $X_0(N)$ maps to $E_1 \times E_2$, which is an abelian surface with elevated NS rank, which ought to provide a quadratic function in the sense of Padma Srinivasan's talk on $X_0(N)$. Does this story have a good "meaning" in terms of the arithmetic E_1 and E_2? (This is more of a vague gesture than an actual question I know!)

David Zureick-Brown. Another quadratic Chabauty challenge (not cursed though): the "next" modular curve to consider is $X_{ns}(17)$. It has genus 6, and its Jacobian breaks up as $A_1 \times A_2 \times A_3$, where the dimension of A_i is i. (The associated newforms are `289.2.a.a`, `289.2.a.b`, `289.2.a.d`) Is this out of reach for quadratic Chabauty? The curve has some rational CM points.

Jackson Morrow. David Cantor has developed a theory of division polynomials for hyperelliptic curves (see here and see here for an article of Robin de Jong expositing them nicely). The theory is very similar to that of elliptic curves in that one uses recursions to define them for arbitrary n. These division polynomials have not been implemented in any compute algebra system, and so the question is can one computationally implement this theory of division polynomials for hyperelliptic curves so that with a click of a button one can get their hands on the n-division polynomial of a given hyperelliptic curve?

There are some immediate difficulties, which were brought up by Nils Bruin. First, the n-torsion scheme on a g-dimensional principally polarized abelian variety does not map in an obvious way to a natural subscheme of $\mathbb{A}^1$, so it is not so easy to write down a univariate polynomial that captures the integral structure uniformly. Second, there is the issue of what to use as parameter space. It may be attractive to parametrize the Jacobian of a hyperelliptic curve $C\colon y^2 = f(x)$ using the coefficients of $f(x)$. For larger primes that works well for the curve, but the Jacobian can have good reduction when the curve does not.

As there seem to be some immediate difficulties, perhaps one can try to write down the division polynomials for hyperelliptic curves of the form $y^2 = x^5 + ax^3 + b$ where $a, b \in \mathbb{Q}^\times$? Or if it makes life easier, let a be the coefficient of some other non-constant term of the defining polynomial.

3. **Additional comments**

Here are some additional comments made during the problem session.

Discussion of Minhyong Kim's contribution.

- There is work of John Pridham (here), which is very relevant to the discussion.

Discussion of Jordan Ellenberg's contribution.

- Davis–Pries–Wickelgren compute this action in the case of Fermat curves, which are maximally symmetric.
- Also, there is work of Anderson–Ihara and Coleman.
- In the case of hyperlliptic curves with a marked rational Weierstrass point, the Ceresa class is trivial.
- For hyperelliptic curves, the thing to look at is the Collino class which is in K_1, and see Wantanabe's thesis for more information.