Explicit methods for rational points on curves

Nils Bruin (Simon Fraser University)
Bjorn Poonen (University of California, Berkeley)

February 4-9, 2007

1 Introduction to the field

One of the "big problems" of number theory is to understand the set of rational points on a variety, or equivalently, the rational solutions to a system of polynomial equations. Despite thousands of years of research, we are very far from having a general method for solving all such problems. There is even some evidence that deciding the existence of a rational solution is an undecidable problem (the corresponding problem for integers, "Hilbert's Tenth Problem", was proved to be undecidable by Martin Davis, Hilary Putnam, Julia Robinson [6]. and Yuri Matijasevič [11]. Therefore many researchers have tried to solve special cases of the general problem.

One way to subdivide the task is to classify varieties by their dimension, which can be defined as the dimension of the complex analytic space whose underlying set is the set of complex number solutions to the system. This space will be a complex manifold if the equations satisfy the differential criterion for smoothness. The study of this complex analytic space is useful for more than just classification: it was discovered in the 20th century that the geometry of this space has a profound influence on the set of rational points.

The rational points on 0-dimensional varieties are easy to understand. By suitable projection, one reduces to the problem of understanding the rational roots of a polynomial in one variable with rational coefficients, and there are elementary methods for understanding these.

Rational points on curves (1-dimensional varieties X) are already much harder: there is still no general algorithm for determining the set of rational points that has been proved to determine the rational points in every case. One can reduce to the case where the curve is smooth, projective, and geometrically integral, or equivalently, where the corresponding complex analytic space is a compact Riemann surface; from now on we will assume this. Then one can subdivide the problem further, according to the topological genus g of the compact Riemann surface. This nonnegative integer g can also be defined algebraically as the dimension of the space of regular differentials, or the dimension of the sheaf cohomology space $H^1(X, \mathcal{O}_X)$.

Major number-theoretic breakthroughs of the 20th century have given us a qualitative understanding of the set $X(\mathbb{Q})$ of rational points on a (smooth, projective, geometrically integral) curve as above. Many of these results generalize to the case where the field $\mathbb{Q}$ of rational numbers is replaced by a finite extension, or even some other types of fields, but for simplicity we will discuss the case of $\mathbb{Q}$.

In the case $g = 0$, the problem of deciding whether $X(\mathbb{Q})$ is nonempty is equivalent to the problem of deciding whether a quadratic form in three variables represents 0, and a criterion for this in terms of congruences goes back to work of Legendre. Moreover, if a rational point exists, then X is isomorphic to the projective line $\mathbb{P}^1$ over $\mathbb{Q}$, and hence the rational solutions may be parametrized. For instance, the special case of (the projective closure of) the curve $x^2 + y^2 = 1$ yields the familiar parametrization of Pythagorean triples.

In the case $g = 1$, it is still not known how to decide whether $X(\mathbb{Q})$ is nonempty. Suppose that $X(\mathbb{Q})$ is nonempty. Then the choice of a point in $X(\mathbb{Q})$ leads to a group structure on the variety X, so $X(\mathbb{Q})$ acquires the structure of an abelian group. The famous Mordell-Weil theorem (due to Mordell in the special case we are considering), proved in the 1920s, states that this group $X(\mathbb{Q})$ is finitely generated. The proof combines a generalization of Fermat's method of infinite descent with a study of the sizes of numerators and denominators of the coordinates of rational points. The Mordell-Weil theorem remains a qualitative result, however, in the sense that there is no algorithm that has been proved to construct generators for this group, or even to calculate the rank of this group. More precisely, researchers have developed algorithms to solve these problems, but these algorithms terminate in general only if for every elliptic curve E over $\mathbb{Q}$, there exists a prime p such that the p-primary part of a torsion abelian group called the Shafarevich-Tate group is finite, as has been conjectured.

In the case $g \geq 2$, Gerd Faltings [7] proved Mordell's 1922 conjecture that $X(\mathbb{Q})$ is finite, and a few years later Paul Vojta [15] gave a completely different proof. But these proofs are ineffective, even in principle: given an explicit curve, the proofs do not give a procedure for listing the rational points: they only (with extra work) give an upper bound for the number of rational points, depending on the input curve. These upper bounds typically appear to be ridiculously large.

There are other techniques that were developed to solve these problems:

1. In some cases, one can determine the rational points on a curve X by finding a non-constant morphism from it to an abelian variety A whose group of rational points is finite; here one often uses the Jacobian J of X, since J is the universal abelian variety through which all morphisms from X to abelian varieties map. If one succeeds in finding such a morphism $X \to A$, one can hope to determine all rational points on A and then examine their preimages in X.

2. If one finds a morphism from X to an abelian variety A such that $A(\mathbb{Q})$ is infinite, but satisfies $\operatorname{rank} A(\mathbb{Q}) < \dim A$, then there is a p-adic analytic method due to Chabauty [3] that provides an upper bound on the number of rational points on X. Moreover, this upper bound is usually reasonable, and often is even sharp, in which case it can be used to determine the set $X(\mathbb{Q})$. The method operates by first computing $A(\mathbb{Q})$ (in fact, one can usually get by with knowledge of a subgroup of finite index therein), and then looking at the intersection of the image of the 1-dimensional p-adic manifold $X(\mathbb{Q}_p)$, with the p-adic closure of $A(\mathbb{Q})$ in $A(\mathbb{Q}_p)$: the latter closure can be shown to be a p-adic analytic submanifold of dimension at most $\operatorname{rank} A(\mathbb{Q})$, so dimension counting suggests that the intersection above is 0-dimensional; Chabauty proved that it was finite, and Robert Coleman [5] showed how to obtain a very explicit upper bound on $\#X(\mathbb{Q})$ via this method.

3. If for every abelian variety quotient A of the Jacobian of X, the inequality $\operatorname{rank} A(\mathbb{Q}) < \dim A$ is violated, then one can try instead ideas originating in work of Chevalley-Weil [4], again generalizing Fermat's infinite descent. One can replace the problem of finding rational points on a given curve X of genus at least 2 with the problem of determining the rational points for a finite set of unramified covers of the given curve. This is often helpful, and it may be that in principle combining this method with Chabauty's method always succeeds in determining the rational points (see [12] and [14], for instance), but in practice, the fact that the covering curves have higher genus than X often makes the computation too time-consuming to carry out to completion. Also, it seems very difficult to prove that this combination of methods would always succeed in principle.

2 Recent developments and open problems

In [8], Minhyong Kim introduced a new idea for studying rational and integral points on curves. Loosely speaking, the Jacobian of a curve classifies geometrically abelian covers of the curve, and Chabauty's method can be understood as applying descent to pass to the tower of geometrically abelian unramified covers of p-power degree. Kim's idea was instead to use the tower of covers coming from the pro-p nilpotent quotient of the algebraic fundamental group of the curve. In direct analogy with Chabauty's method, he defines a "unipotent Albanese map" from $X(\mathbb{Q}_p)$ not to $J(\mathbb{Q}_p)$ but to the p-adic points of a pro-unipotent algebraic group $\pi_{1,DR}(X, x)$. Using this, he gave a new proof of Siegel's theorem on the finiteness of the set of solutions to S-unit equations, for S a finite set of places of $\mathbb{Q}$. Although this particular result can also be

obtained by the more elementary approach of applying Chabauty's method to unramified covers of $\mathbb{P}^1 - \{0, 1, \infty\}$, it seemed possible that Kim's method might be applicable to other situations for which it is not clear that applying Chabauty's method to unramified covers would work. As evidence for this, Kim showed that various conjectures (about Galois cohomology or Galois representations) would imply that his technique would prove the finiteness of the set of integral points on any hyperbolic curve over $\mathbb{Q}$, and in particular the finiteness of the set of rational points on any smooth projective curve of genus at least 2 over $\mathbb{Q}$.

This raises several questions:

1. Is it actually the case that Kim's approach is equivalent to Chabauty's approach applied to unramified covers? If not, is one approach stronger than the other?

2. Does Kim's approach lead to a new proof of Faltings' theorem in general?

3. Does Kim's approach suggest an algorithm, along the lines of the algorithm that implements Chabauty's ideas?

One of the main goals of the workshop was to bring people together to try to gain insight on these difficult questions.

3 Workshop presentations

3.1 Expository talks

Tim Dokchitser – *Analytic ranks of Jacobians of curves*

This talk concentrated on a conjectural but, if ever proven, very powerful way of computing the free rank of abelian varieties over the rational numbers.

One associates to any Abelian variety over the rationals an analytic object, its *L-series*. This is an analytic function in, say, s, defined by a convergent series for $\mathrm{Re}(s) > 3/2$. According to a conjecture by Birch and Swinnerton-Dyer, this function extends to a meromorphic function on the entire complex plane, and the order of vanishing at $s = 1$ should correspond to the free rank of the group of rational points on the abelian variety. Furthermore, the lowest order derivative that does not vanish should take a value at $s = 1$ which is a combination of virtually all interesting arithmetic geometric quantities associated to the abelian variety. In particular, the conjectural order of the Shafarevich-Tate group can be read off from that value.

In practice, even getting a complete description of the L-series can be troublesome, because some of the relevant arithmetic information that makes up the L series is hard to compute. Using even further conjectures, one can often make an educated guess about this information. In this talk, the speaker showed how to apply these ideas in practice . He demonstrated how his newly developed software in the computer algebra system MAGMA can be used and showed some impressive examples. One of the highlights was a genus 3 curve, for which he conjectured that the Jacobian should be of rank 5.

An interesting question raised by his talk is whether algebraic methods (e.g., 2-descent on the Jacobian of this genus 3 curve) can obtain this result. Some of the participants thought about this for a while, and could not see an easy way to do it. So at least for the time being, it seems as the analytic approach and the algebraic approach complement each other, each able to contribute information that might be inaccessible via the other approach.

William McCallum – *Introduction to explicit Chabauty methods*

Given that one of the main themes of this workshop was *non-Abelian Chabauty* - a generalisation of Chabauty's original method to obtain a partial proof of Mordell's conjecture, the organizers invited one of the experts on the method to give a lecture series on the introduction into the original idea.

Let C be a complete, irreducible, nonsingular algebraic curve over the field of rational numbers, of genus at least 2. Suppose we have a degree 1 divisor class on C. We can use that to consider C as a subvariety of the Jacobian J of C. Hence, the rational points of C can be considered a subset of the rational points of J.

We consider $J(\mathbb{Q}) \subset J(\mathbb{Q}_p)$. for some prime p. A nice property of p-adic analytic commutative lie-groups is that a finitely generated subgroup of rank r is contained in an analytic submanifold of dimension

at most r. Hence, if $J(\mathbb{Q})$ is of rank strictly lower than the dimension of J, then it is contained in a proper submanifold $\overline{J(\mathbb{Q})} \subset J(\mathbb{Q}_p)$.

We can then find a bound on $\#C(\mathbb{Q})$ via the inclusion $C(\mathbb{Q}) \subset C(\mathbb{Q}_p) \cap J(\mathbb{Q})$. The latter is an intersection of a 1-dimensional $\mathbb{Q}_p$-analytic algebraic variety with a proper p-adic analytic submanifold of the ambient space. One would expect a 0-dimensional (in fact finite) intersection and one can show that this is indeed the case. The cardinality of this analytic intersection provides an upper bound on $C(\mathbb{Q})$.

In this talk, it is explained how all analytic computations can be formulated in terms of p-adic integration on the curve and several well-known examples from the literature are explained and demonstrated.

Several modifications of the method, in particular the use of covers and replacing J (if possible) with a computationally more accessible Weil-restriction of an elliptic curve are also mentioned.

Edward Schaefer – *Bounding the Mordell-Weil rank of the Jacobian of a curve*

A crucial ingredient for the application of Chabauty's method to a curve C over $\mathbb{Q}$ with Jacobian J, is a detailed knowledge of $J(\mathbb{Q})$, the Mordell-Weil group. In particular, one needs to know the free rank of this group.

One can read off this rank from a quotient $J(\mathbb{Q})/pJ(\mathbb{Q})$. The method of *descent* tries to approximate this group by a group that is quaranteed to contain the given group, the p-Selmer group of J. The cardinality of the latter thus provides an upper bound on the cardinality of the former, and thus implies a bound on the Mordell-Weil rank of J.

The talk explains in detail how the general Galois-cohomological framework one can use to describe the required objects can be translated into explicitly computable objects.

As a particular example, a famous historical computation is repeated, thus providing the required information to complete the argument given in McCallum's talk.

Michael Stoll – *Local-global obstructions, coverings, and Mordell-Weil sieving*

If Chabauty's method applies, i.e., if $J(\mathbb{Q})$ is of smaller rank than the dimension of J, then it provides a proof that $C(\mathbb{Q}) \to J(\mathbb{Q})/NJ(\mathbb{Q})$ is injective for some explicit N. It then remains to determine which classes in $J(\mathbb{Q})/NJ(\mathbb{Q})$ do contain a rational point.

As it turns out, assuming we can consider C as a subvariety of J, considering the intersection of the image of $J(\mathbb{Q})$ in $\prod_{p\in S} J(\mathbb{F}_p)$ with $\prod_{p\in S} C(\mathbb{F}_p)$ for some suitably chosen set of primes S provides quite strong congruence information on the image of $C(\mathbb{Q})$ in $J(\mathbb{Q})$. In fact, heuristically (see [13]), one expects that once should be able to get accurate information for any N. The procedure of obtaining such information is now known as *Mordell-Weil sieving*.

In particular, the same heuristics predict that using this procedure for a curve C that does not have rational points, one should be able to show this using a suitably chosen set S.

This talk explains this procedure and its link with the idea of using coverings as in [4] and the Brauer-Manin obstruction in general.

3.2 Talks on non-abelian Chabauty

Richard Hain – *Higher Albanese Manifolds*

This talk explains the construction of *higher albanese manifolds* in the complex analytic situation. The same construction is used in a p-adic setting for Kim's non-abelian Chabauty.

The usual complex analytic Albanese variety of a curve C may be defined by integrating holomorphic 1-forms along paths on the complex Riemann surface corresponding to the curve. These provide functions on the path space of C that are defined on classes of paths modulo the commutator of the fundamental group, and equip this quotient with a manifold structure.

For higher albanese varieties, one replaces the integrals by *iterated* integrals as studied by Chen. These are defined only on path classes modulo terms from the lower central series of the fundamental group. This talk gave an overview of this construction, including Chen's theorem relating the pro-unipotent completion of the fundamental group with the Hopf algebra of homotopy functionals.

Kiran Kedlaya – *p-adic Hodge Theory*

This talk provided an introduction into p-adic Hodge theory. Given a smooth proper scheme X over $\mathbb{Z}_p$, one has the p-adic étale cohomology of its base extension to $\overline{\mathbb{Q}}_p$ and its de Rham cohomology with $\mathbb{Q}_p$-coefficients. Comparison theorems proved by Faltings and Tsuji describe how one can recover either of these cohomology spaces from the other by using Fontaine's "big ring" B_{crys}. They allow one to compare the p-adic integration map from a curve to the Lie algebra of its Jacobian over $\mathbb{Q}_p$ with a cohomologically defined map. The results described so far belong to abelian p-adic Hodge theory. The talk ended with a brief sketch of some non-abelian generalizations.

Minhyong Kim – Non-abelian Chabauty

Chabauty's original partial proof of Mordell's Conjecture (now Faltings' Theorem) on finiteness of the number of rational points on algebraic curves of genus at least 2 is based on considering the curve as a subvariety of an abelian variety. Since the Albanese variety is universal with respect to that property, no generality is lost by considering the curve as a subvariety of the Albanese. Chabauty's argument is based on the assumption that the rational points of the Albanese lie in a proper p-adic submanifold. This assumption does not hold in general.

One can try to use larger group varieties — non-abelian ones. The higher Albanese varieties are some of the next simplest examples, being unipotent. The hope is that even in the case where the rational points in the classical Albanese variety lie p-adically dense, we can find a higher Albanese where the rational points do lie in a proper submanifold.

For non-complete hyperbolic curves — in particular $\mathbb{P}^1$ over $\mathbb{Z}$ minus 3 points — Kim was able to prove that this is indeed the case. He was thus able to recover Siegel's result on finiteness of the number of solutions to S-unit equations [8]. He has also shown that various "motivic conjectures," such as the Bloch-Kato conjecture on surjectivity of p-adic Chern class maps or the Fontaine-Mazur conjecture on representations of geometric origin, would imply that his method reproves the theorems of Faltings and Siegel for hyperbolic curves over $\mathbb{Q}$ [9].

In his series of talks, Kim explained the construction he used, with the express purpose of looking whether this method can be made explicit and perhaps be used to produce actual bounds on the number of solutions. The progress made during the workshop shows that this may indeed be the case.

After giving some motivating examples, he explained the map (arising in Grothendieck's section conjecture) from the set of rational points on a variety to the Galois cohomology H^1 of its fundamental group over $\overline{\mathbb{Q}}$, and then he discussed the version of this for the pro-unipotent completion of the fundamental group, and finally connected this with the de Rham picture in which p-adic iterated integrals play a key role.

3.3 Research talks

Abstracts of all but one of the research talks are given in Appendix B below. We provide a summary of the talk for which no abstract was provided.

Iftikhar Burhanuddin – *Brauer-Siegel Analogue for Elliptic Curves over the Rationals*

See abstract.

Jordan Ellenberg – *Obstructions to rational points on curves coming from the nilpotent geometric fundamental group*

In this talk another interesting obstruction arising from the nilpotent fundamental group is discussed. It is torsion, so this obstruction is invisible for the uniponent Albanese construction used by Kim, who tensors with $\mathbb{Q}_p$. As a special example, for $\mathbb{P}^1$ minus three points, the ordinary quadratic Hilbert symbol was recovered.

The talk was a report on ongoing research. No explicit new results could be reported on yet.

Florian Hess – *Explicit generating sets of Jacobians of curves over finite fields, using some class field theory*

See abstract.

Catherine O'Neil – *Trilinear forms and elliptic curves*

See abstract.

Samir Siksek – *Chabauty for Symmetric Powers of Curves*

See abstract.

William Stein – ***Explicitly computing information about Shafarevich-Tate groups of elliptic curves using L-functions, Euler systems, and Iwasawa theory***
See abstract.

Michael Stoll – ***Rational points on small curves of genus 2 - an experiment***
See abstract and [2].

Ronald van Luijk – ***Cubic points on cubic curves and the Brauer-Manin obstruction for K3 surfaces***
See abstract.

4 The impact of the workshop

Here we describe some new collaborations, projects, and success stories that came into being because of our workshop. Some of these took place during the workshop itself; in other cases, participants told us a few weeks later about progress that had ensued.

- Jordan Ellenberg, Richard Hain, Minhyong Kim, and Kirsten Wickelgren (a graduate student) began a new collaboration in order to compute the "Selmer varieties", which are the analogue of the p-adic closure of the Mordell-Weil group, in Chabauty's method. The computation of these varieties seems to be the most difficult part of Kim's approach, the main obstacle to making the approach a viable method. Yes, on Thursday night of the workshop, they made significant progress! This group of researchers also hopes to study a characteristic-zero function field analogue.

- Kirsten Wickelgren writes also that during the workshop Minhyong Kim made an observation about a map that she now uses to compute examples for her Ph. D. thesis.

- Richard Hain, a topologist who is an expert in the theory of iterated integrals and pro-unipotent fundamental groups in the classical case (as opposed to the p-adic case used in Kim's work) wrote that during the course of the workshop he went from having little understanding of Kim's program to having a good grasp of it. As a result, he and Kim are going to write a updated exposition of some of the key topological ideas, but with an eye towards applications to Kim's program. In particular, they will treat iterated integrals on algebraic curves, iterated Coleman p-adic integration, computing the Hodge filtration via the pole integration. Some of these topics have not been fully developed even in the research literature, so their new exposition will be very welcome.

- Iftikhar Burhanuddin (a graduate student) wrote that he received valuable feedback in response to his workshop talk on an elliptic curve analogue of the Brauer-Siegel theorem, and that this feedback is guiding the computational data that he will collect for his Ph. D. thesis.

- At the workshop, a small subset of the participants met to discuss the issue of implementing the computation of p-adic iterated integrals, a necessary step in making Kim's approach practical. Kiran Kedlaya, who was scheduled to deliver a lecture series for graduate students and lead them in a project at the Arizona Winter School this year, wrote that the workshop gave him the idea of involving the students in a project along these lines. At the workshop, we were discussing only the case of good reduction, but Kedlaya has been led to begin investigating the more general case of semistable reduction as well.

- Nils Bruin, Bjorn Poonen, and Michael Stoll stayed one extra day at BIRS; during that day, they worked together on developing explicit 2-descent for general curves of genus 3. Significant progress was made, showing that the computations required could be reduced to the point of almost being doable with current computing power and class group algorithms (modulo the Generalized Riemann Hypothesis). In fact, a few weeks later, we had our first success along these lines, albeit for a curve with very small discriminant.

In addition, many participants, both those studying computational number theory and those involved in more theoretical aspects, wrote to us expressing their thanks for the opportunity to learn about the new ideas that were in the process of being developed. Despite some of the subject matter being highly technical, having experts present who could explain things in a friendly learning environment led to many people leaving with a good sense of the issues involved.

5 For more information

A more extensive account of the presentations given in this workshop can be found on the website

`http://www.cecm.sfu.ca/~nbruin/banff2007`

For nearly all talks, either copies of the slides used or extensive notes taken by Bjorn Poonen are available. Links to preprints and further reading are also accessible.

Appendix A: List of participants

1. Burcu Baran, University of Rome Tor Vergata
2. Ioan Berbec, University of California at Berkeley
3. Martin Bright, University of Bristol
4. Reinier Bröker, Fields Institute
5. David Brown, University of California at Berkeley
6. Nils Bruin, Simon Fraser University
7. Iftikhar Burhanuddin, University of Southern California
8. Robert Carls, University of Leiden
9. Imin Chen, Simon Fraser University
10. Henri Cohen, Universite Bordeaux 1
11. Robert Coleman, University of California at Berkeley
12. Jean-Marc Couveignes, Université Toulouse II, Groupe de Recherche en Informatique et Mathématiques (GRIMM)
13. Tim Dokchitser, Robinson College, Cambridge
14. Jordan Ellenberg, University of Wisconsin
15. Richard Hain, Duke University
16. Florian Hess, Technische Universität Berlin
17. Kiran Kedlaya, Massachusetts Institute of Technology
18. Minhyong Kim, University of Arizona and Purdue University
19. Abhinav Kumar, Microsoft Research
20. Adam Logan, University of Waterloo
21. William McCallum, University of Arizona
22. Catherine O'Neil, Barnard College, Columbia University

23. Jennifer Paulhus, University of Illinois at Urbana-Champaign
24. Bjorn Poonen, University of California at Berkeley
25. Ed Schaefer, Santa Clara University
26. René Schoof, University of Rome II
27. Samir Siksek, University of Warwick
28. William Stein, University of Washington
29. Michael Stoll, International University Bremen
30. Ronald van Luijk, PIMS, SFU, UBC
31. John Voight, University of Minnesota
32. Mark Watkins, University of Bristol
33. Joseph Wetherell, Center for Communications Research
34. Kirsten Wickelgren, Stanford University

Appendix B: Schedule of the workshop

Monday, February 5, 2007

9:00 – 9:10 Introduction to BIRS

9:10 – 10:00 William McCallum – *Introduction to explicit Chabauty methods I*

10:30 – 11:20 William McCallum – *Introduction to explicit Chabauty methods II*

2:30 – 3:20 Richard Hain – *Higher Albanese Manifolds*

4:00 – 4:50 Kiran Kedlaya – *p-adic Hodge Theory*

> At the request of the organizers, I will introduce/review some constructions from p-adic Hodge theory that intervene in the usual Chabauty method; these include the comparison isomorphism between the de Rham and etale cohomology groups of a curve, and the Bloch-Kato exponential map. I will focus on the case of good ordinary reduction, where these constructions can be made reasonably explicit. The goal is to analogize the explicit descriptions to the higher unipotent de Rham and etale fundamental groups, in a manner useful for doing nonabelian Chabauty; as time and my abilities permit, I will start doing this (again only in the good reduction case) using some work of Martin Olsson.

Tuesday, February 6, 2007

9:10 – 10:00 Minhyong Kim, I

10:30 – 11:20 Minhyong Kim, II

2:30 – 3:20 Edward Schaefer – *Bounding the Mordell-Weil rank of the Jacobian of a curve*

> We use a Chabauty computation to determine the set of rational points on a curve of higher genus. The input for a Chabauty computation includes the Mordell-Weil rank of the associated Jacobian. Traditionally we bound, and hope to determine, the Mordell-Weil rank using a Selmer group. In this talk, we will survey the methods for computing a Selmer group of a Jacobian using functions on the curve. We will review both major methods. The first is quite general, but is inefficient for cyclic covers of the projective line (like hyperelliptic curves). The second method addresses such covers.

4:00 – 4:50 Michael Stoll – *Local-global obstructions, coverings, and Mordell-Weil sieving*

We will discuss how one can obtain information on rational points by combining coverings with local information. We will focus on the case of abelian coverings and explain the relationship with the Brauer-Manin obstruction. If explicit generators of the Mordell-Weil group are known, this can be implemented efficiently, leading to a procedure known as the Mordell-Weil sieve. We will formulate a conjecture that, if valid for a given curve, implies that we can effectively decide whether a given coset of N times the Mordell-Weil group meets the image of the curve or not. If we know that each such coset contains at most one point coming from the curve, this means that we can determine the set of rational points on the curve.

5:00 – 5:50 Jordan Ellenberg – *Obstructions to rational points on curves coming from the nilpotent geometric fundamental group*

Wednesday, February 7, 2007

8:40 – 9:30 Minhyong Kim, III

9:40 – 10:30 Samir Siksek – *Chabauty for Symmetric Powers of Curves*

Let C be a curve of genus $g \geq 3$ and let $C^{(d)}$ denote its d-th symmetric power. We explain an adaptation of Chabauty which allows us in many cases to compute $C^{(d)}(\mathbb{Q})$ provided the rank of the Mordell-Weil group is at most $g - d$. Cases for which our method should work include:

(i) $d < \gamma$ where γ is the gonality of C and the jacobian is simple (here $C^{(d)}(\mathbb{Q})$ is finite).

(ii) C is hyperelliptic and $d = 2$ (here $C^{(d)}(\mathbb{Q})$ is infinite).

(iii) C is bielliptic and $d = 2$ (here $C^{(d)}(\mathbb{Q})$ can be infinite). Our adaptation of Chabauty differs from the classical Chabauty in that we combine Chabauty type information given by several primes.

Example. Let C be the genus 3 hyperelliptic curve

$$C : y^2 = x(x^2 + 2)(x^2 + 43)(x^2 + 8x - 6) \tag{1}$$

with Jacobian having rank 1. Let $\pi : C \to P^1$ be the x-coordinate map. We show that $C^{(2)}(\mathbb{Q})$ consists of $\pi^{-1}P^1(\mathbb{Q})$ plus 10 other points which we write down explicitly. Here we needed to combine the Chabauty information at primes $p = 5, 7, 13$. It is noteworthy that $C^{(2)}$ in this example is a surface of general type.

Thursday, February 8, 2007

9:10 – 10:00 Tim Dokchitser – *Analytic ranks of Jacobians of curves*

10:30 – 11:20 Ronald van Luijk – *Cubic points on cubic curves and the Brauer-Manin obstruction for K3 surfaces*

It is well-known that not all varieties over $\mathbb{Q}$ satisfy the Hasse principle. The famous Selmer curve given by $3x^3 + 4y^3 + 5z^3 = 0$ in $\mathbb{P}^2$, for instance, indeed has points over every completion of $\mathbb{Q}$, but no points over $\mathbb{Q}$ itself. Though it is trivial to find points over some cubic field, it is a priori not obvious whether there are points over a cubic field that is galois. We will see that such points do exist. K3 surfaces do not satisfy the Hasse principle either, which in some cases can be explained by the so called Brauer-Manin obstruction. It is not known whether this obstruction is the only obstruction to the existence of rational points on K3 surfaces. We relate the two problems by sketching a proof of the following fact. If there exists a smooth curve over $\mathbb{Q}$ given by $ax^3 + by^3 + cz^3 = 0$ that is locally solvable everywhere, that has no points over any cubic galois extension of $\mathbb{Q}$, and whose Jacobian has trivial Mordell-Weil group, then the algebraic part of the Brauer-Manin obstruction is not the only one for K3 surfaces. No knowledge about K3 surfaces or Brauer-Manin obstructions will be assumed as known.

2:30 – 3:20 Catherine O'Neil – *Trilinear forms and elliptic curves*

We explain a correspondence between triliear forms and triples of genus one curves with a fixed Jacobian and some added structure. We generalize the addition law on elliptic curves to addition on certain "cubes" of numbers. We explain how this works for arbitrary rings, and we give a natural construction of points on elliptic curves to other points on other elliptic curves which generalizes a known construction from class field theory.

4:00 – 4:50 William Stein – *Explicilty computing information about Shafarevich-Tate groups of elliptic curves using L-functions, Euler Systems, and Iwasawa theory*

I will discuss theoretical and computational results toward the following problem: given a specific elliptic curve over $\mathbb{Q}$, compute the exact order and structure of its Shafarevich-Tate group in practice. I view this problem as a motivating question for organizing both theoretical and algorithmic investigations into the arithmetic of elliptic curves and the Birch and Swinnerton-Dyer conjecture.

5:00 – 5:30 Iftikhar Burhanuddin – *Brauer-Siegel Analogue for Elliptic Curves over the Rationals*

The height of a rational point on an elliptic curve measures the size of the point. The enormous gap between the lower and upper bound (Lang's conjectures) of the height of such a point, prompted the comparison of the elliptic curve scenario with that of the multiplicative group, the Brauer-Siegel theorem. In this talk, a conjectural Brauer-Siegel theorem for elliptic curves over the rationals will be discussed and interesting questions which arise in this context motivated by computation will be presented.

Friday, February 9, 2007

9:10 – 10:00 Florian Hess – *Explicit generating sets of Jacobians of curves over finite fields, using some class field theory*

10:30 – 11:20 Michael Stoll – *Rational points on small curves of genus 2 - an experiment*

We considered all genus 2 curves $y^2 = f(x)$ where f has integral coefficients of absolute value at most 3; there are about 200,000 isomorphism classes of such curves. Using various methods (point search, local solubility, 2-descent, Mordell-Weil sieve), we attempted to decide for each curve whether it possesses rational points. In all but 42 cases, we were successful; in the remaining cases, our result is conditional on the Birch and Swinnerton-Dyer conjecture. In the talk, we will explain the methods we used and the improvements we came up with, and discuss the results.

References

[1] N. Bruin and B. Poonen, workshop website, 2007, `http://www.cecm.sfu.ca/~nbruin/banff2007`.

[2] N. Bruin and M. Stoll, Rational points on small curves of genus 2 – an experiment, preprint, 2006, `http://arxiv.org/abs/math.NT/0604524`.

[3] C. Chabauty, Sur les points rationnels des courbes algébriques de genre supérieur à l'unité, *C. R. Acad. Sci. Paris* **212** (1941), 882–885.

[4] C. Chevalley and A. Weil, Un théorème d'arithmétique sur les courbes algébriques, *Comptes Rendus Hebdomadaires des Séances de l'Acad. des Sci., Paris* **195** (1930), 570–572.

[5] R. Coleman, Effective Chabauty, *Duke Math. J.* **52** (1985), 765–770.

[6] M. Davis, H. Putnam, J. Robinson, The decision problem for exponential diophantine equations, *Ann. of Math. (2)* **74** (1961), 425–436.

[7] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, *Invent. Math.* **73** (1983), 349–366. Translation: Finiteness theorems for abelian varieties over number fields in *Arithmetic geometry (Storrs, Conn., 1984)*, 9–27. Erratum: *Invent. Math.* **75** (1984), 381.

[8] M. Kim, The motivic fundamental group of $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel, *Invent. Math.* **161** (2005), 629–656.

[9] M. Kim, The unipotent Albanese map and Selmer varieties for curves, preprint, 2005, `http://arxiv.org/abs/math.NT/0510441`.

[10] M. Kim and A. Tamagawa, The l-component of the unipotent Albanese map, preprint, 2006, `http://arxiv.org/abs/math.NT/0611384`.

[11] J. Matijasevič, The Diophantineness of enumerable sets, *Dokl. Akad. Nauk SSSR* **191** (1970), 279–282.

[12] B. Poonen, Computing rational points on curves. In *Number theory for the millennium, III (Urbana, IL, 2000)*, 149–172, A K Peters, 2002.

[13] B. Poonen, Heuristics for the Brauer-Manin obstruction for curves, *Experimental Math.* **15** (2006), 415–420.

[14] M. Stoll, Finite descent obstructions and rational points on curves, preprint, 2006, `http://arxiv.org/abs/math.NT/0606465`.

[15] P. Vojta, Siegel's theorem in the compact case, *Ann. of Math. (2)* **133** (1991), 509–548.