The Cohen-Lenstra heuristics for class groups

The American Institute of Mathematics

The following compilation of participant contributions is only intended as a lead-in to the AIM workshop “The Cohen-Lenstra heuristics for class groups.” This material is not for public distribution.

Corrections and new material are welcomed and can be sent to workshops@aimath.org

Version: Wed Jun 8 18:21:44 2011

Table of Contents

Chapter A: Participant Contributions

A.1 Conrad, Brian

I know a fair bit about algebraic groups and algebraic geometry and algebraic number theory, so I think I should be able to contribute useful suggestions in the discussions, in whatever form they may take (working groups, open problem discussion, etc.). I don't have prior experience with Bhargava's work, but have seen some talks on it and expect that I know enough that I can pick things up pretty quickly.

A.2 Delaunay, Christophe

Fix an elliptic curve $E/\mathbb{Q}$ and suppose the E has minimal conductor among its quadratic twists. Consider a natural family $\mathcal{F}$ of rank 0 (imaginary) quadratic twists of E (in the sequel, we note E_d the quadratic twist of E by d). Fix a prime p, if the prime p is "nice" for $\mathcal{F}$, then the heuristics on Tate-Shafarevich groups predict precisely the frequency of $|Sha(E_d)|$ that are divisible by p. It would be interesting to investigate more precisely the condition "nice" for p relatively to E, in particular for the prime $p = 2$. Indeed, numerical investigations confirm the predictions of the heuristics and the odd nice primes seem to be the odd primes that do not divide $|E(\mathbb{Q})_{\text{tors}}|$ (in particular, p should be nice if $p > 7$). For an odd prime p dividing $|E(\mathbb{Q})_{\text{tors}}|$, then the frequency of $|Sha(E_d)|$ divisible by p should be rather given by the original Cohen-Lenstra heuristics for class groups of imaginary quadratic fields. Several works had been done in the direction of this observation (Quattrini, Wong,...). A natural question is what happens for $p = 2$? In that case, numerical results are far from the predictions but it appears that the 2-part of the Tate-Shafarevich groups $Sha(E_d)$ acquire their normal behavior for large d. On the other hand, if E has complete 2-torsion and no cyclic subgroup of order 4 defined over $\mathbf{Q}$, then P. Swinnerton-Dyer followed by D. Kane obtained theoretical results about the rank of the 2-Selmer groups of E_d that agree exactly with the heuristics on *Sha*. Would it be possible to investigate such results about the 2-Selmer groups whenever E has complete 2-torsion and a cyclic subgroup of order 4 torsion defined over $\mathbf{Q}$? What happens if E has no complete 2-torsion defined over $\mathbb{Q}$?

References:

P. Swinnerton-Dyer, *The effect of twisting on the 2-Selmer group*, Math. Proc. Camb. Phil. Soc., vol. 145, 3, 513–526.

D. Kane, *On the Ranks of the 2-Selmer Groups of Twists of a Given Elliptic Curve*, arXiv:1009.1365v2.

A.3 Elkies, Noam

I have some experience with the relevant spaces from my own work with explicit moduli, descents on elliptic curves and surfaces, and other objects in arithmetic geometry. Heuristics for ranks of elliptic curves and higher abelian varieties (or Neron-Severi groups) also figure into my searches for Diophantine records for high ranks, curves with many points, etc.

A.4 Ellenberg, Jordan

The focus of my recent work with Venkatesh and Westerland has been to understand geometric structures that explain, and prove some results towards, Cohen-Lenstra and Cohen-Lenstra-Martinet conjectures over the field $F_q(t)$. It turns out that the relevant geometric input comes from topology, involving stabilization theorems for the cohomology of various moduli spaces, especially Hurwitz spaces.

A couple of topics I would like to think about at the meeting:

- Many asymptotic arithmetic questions can be expressed, in the function field case, in terms of stable cohomology of Hurwitz spaces with coefficients in local systems other than the trivial one. This brings us into contact with very recent work of Church and Farb on "representation stability," which seems to be relevant to questions like "Is Cohen-Lenstra true when restricted to prime discriminant?" or "What is the right conjecture for the distribution of Iwasawa lambda-invariants?" (One proposed answer to the second question is found in a paper I wrote with Jain and Venkatesh.)
- "p-adic Cohen-Lenstra" – Cohen-Lenstra tells you what the p-torsion group scheme of a random hyperelliptic curve over F_ℓ looks like, but what about a random hyperelliptic curve over F_p? For instance, what is the probability that a random curve is ordinary? I have some work in progress on this with David Brown and Bryden Cais, and would be very interested to get more insight into this problem from people at the workshop.
- To what extent can Cohen-Lenstra conjectures be thought of as l-adic analogues of the random matrix conjectures for the zeroes of L-functions? (This is the train of thought that starts with Friedman-Washington and proceeds through Yu, Achter, Garton, etc.)

A.5 Fouvry, Etienne

In several papers with J. Klueners,(see MathSciNet for references) we proved several results going in the direction of the truth of the Cohen-Lenstra heuristics (extended by Gerth) for the 4-rank of quadratic fields, real or imaginary. In some sense, the question of the 4-rank is now solved and had applications for the counting problem of real quadratic fields with fundamental unit with negative norm. However, as a by-product, we found some result on the distribution of the 8-rank, and only for fundamental discriminants with all their prime factors congruent to 1 modulo 4. I think the question of the 8-rank is attractive to see which tools from algebraic number theory will be used and to guess whether analytic number theory is strong enough to understand the asymptotic behavior of these tools.

Secondly, with F. Jouve, we investigated the size of the fundamental solution of Pell equation $x^2 - Dy^2 = 1$, following a paper of C. Hooley (Crelle 1984). We found several improvements of Hooley's results. Here also, we are quite interested by the analytic tools which are incorporated (exponential sums, sieves) Actually, our purpose is to improve the lower and upper bounds of the sum

$$S(X) := \sum_{D \leq X} h(D),$$

where $h(D)$ is the class number associated to the discriminant D (not necessarily fundamental). The preprints concerning these results can be found on my personal webpage.

A.6 Klagsbrun, Zev

My current research interest is Selmer ranks of quadratic twists of elliptic curves. The primary question I am focusing on is given an elliptic curve E/K, what is the distribution of 2-Selmer ranks within the family of all quadratic twists of E? This question has been answered by Heath-Brown, Swinnerton-Dyer, and Kane for all elliptic curves over $\mathbb{Q}$ with

$E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. While Mazur, Rubin, and Klagsbrun have obtained some results for the cases when $E(K)[2] = 0$ and $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$, the question still remains open for these cases.

Additionally, I am interested in learning about the Cohen-Lenstra heuristics with an interest in seeing if any of the lessons learned from my work on Selmer groups can be applied to ideal class groups.

A.7 Lagemann, Thorsten

Currently, I am working on the asymptotic of Galois groups over global or local function fields, where the characteristic of the given field divides the order of the given group. I have interests in the cross references with the Cohen-Lenstra heuristic (CLH), and the CLH on function fields in general.

A.8 McGown, Kevin

In June of 2010 I completed my Ph.D. under the supervision of Harold Stark at U.C. San Diego and I am currently a postdoc at Oregon State University in Corvallis, Oregon. I work in the intersection of algebraic and analytic number theory, and my main area of research has been Euclidean number fields.

I developed an interest in the Cohen–Lenstra heuristics in graduate school and have read a little of the early literature on the subject. I am very interested in learning more, including what recent progress has been made and what the current avenues of research are. I can see this as a potential direction of research for myself, and I am very eager to collaborate on open problems.

At least from a naive point of view, I feel that the study of norm-Euclidean fields is, in many ways, analogous to the study of class number one fields – in some situations we can prove that there are only finitely many norm-Euclidean fields, while in others we expect that there are infinitely many, but cannot prove so. For example, there are only finitely many norm-Euclidean real quadratic fields, but we suspect there to be infinitely many norm-Euclidean totally-real cubic fields.

However, unlike in class number problems, insofar as I know, we don't even have a heuristic as to how many fields we should expect to be norm-Euclidean. One possible question: Is there a heuristic (preferably quantifiable) "reason" that there should be (or not be) infinitely many norm-Euclidean fields when the unit rank is greater than or equal to two? It would be very desirable to have such a heuristic if one doesn't already exist.

A.9 Roberts, David

I am interested in the general topic of mass heuristics for the number of number fields with say a given discriminant and a given Galois group. While the Cohen-Lenstra heuristics in their classical form are about unramified abelian extensions, I am interested in the general case of extensions with arbitrary Galois group and arbitrary prescribed ramification. In the past several years I have found extensions which are surprising from the point of view of the current mass heuristics, for example a degree 15875 extension with discriminant of the form -2^a5^b and Galois group all of S_{15875}. I would like to develop a conceptual framework for such exceptional fields.

I am interested also in low degree cases where theoretical considerations can be compared with experiment. For example, with John Jones I have recently computed all totally real A_5 quintics with discriminants $\leq 2^38$, extending a computation of Malle who went out through 2^37. Of the fields with discriminant of the form p^2, we found that 186 have ramification type $(2, 2, 1)$ while 556 have ramification type $(3, 1, 1)$. Naively, one might might have expected a ratio of $1 : 1$ while Ellenberg and Venkatesh predicted an asymptotic ratio of $1 : 2$. Through our cutoff, the ratio is almost exactly 1:3. Again, I would like a conceptual understanding of this: is there a secondary term at work here?

A.10 Thorne, Frank

My primary interest, as it relates to this workshop, is in the theory of the zeta functions associated to prehomogeneous vector spaces, developed by Sato and Shintani.

In collaboration with Takashi Taniguchi, I refined Davenport-Heilbronn's asymptotic formula for 3-torsion in quadratic fields, and obtained a power-saving error term as well as a secondary main term. Taniguchi and I proved a similar result for cubic fields (as did Bhargava, Shankar, and Tsimerman), and proved generalizations to arithmetic progressions. The arithmetic progressions case is particularly interesting, as there is an unexpected bias; for example, there is more 3-torsion in quadratic fields whose discriminant is congruent to 1 (mod 7) than those whose discriminant is 2 (mod 7).

This has connections to a variety of other work. In the first place, the Sato-Shintani theory applies to any prehomogeneous vector space, although in general most of the technical computations (e.g. residue formulas) are not in place. As such, it can be used to study any aspect of the Cohen-Lenstra heuristics which correspond to prehomogeneous vector spaces. Moreover, it might be possible that the theory can be generalized to the sorts of "coregular" spaces being investigated by Bhargava and his collaborators. I know little about this now, but it would be interesting to learn more.

More generally speaking, my background is in analytic number theory and I am familiar with standard techniques such as sieving and estimating partial sums of Dirichlet series.

A.11 Westerland, Craig

First a caveat: I am a topologist. My background in the Cohen-Lenstra heuristics is in the function field setting, where it is rephrased as a counting problem for branched covers of curves with specified monodromy and ramification data. Some computations in this setting can be performed using homological stability results for Hurwitz moduli spaces of such covers. In joint work with Jordan Ellenberg and Akshay Venkatesh, we have used these techniques to prove versions of the heuristics for imaginary quadratic extensions of $\mathbb{F}_q(t)$.

There are two main topological components of these results. The first is a *homological stability theorem* that ensures that the rational cohomology of these Hurwitz spaces stabilizes as the number of branch points grows. The second is a computation of what these stable cohomology groups actually are. These results are then fed into the Grothendieck-Lefschetz fixed point theorem to produce an estimate of the number of points of these moduli spaces (that is, covers with specified mondromy data). This estimate improves as the number of branch points tends to infinity (thanks to the stability theorem), giving the answer predicted by the Cohen-Lenstra heuristics.

We have achieved a stability theorem only in the case relevant to the imaginary quadratic extensions, whereas we we can compute the limiting (if not stable) homologies for all manner of Galois groups. Proving stability for other Galois groups should yield similar results. Pursuing homological stability for general Galois groups would be an interesting problem (for me at least) to examine at the workshop.

Another subject of interest is the following: much of the techniques for computing the limiting homology of Hurwitz spaces works for general moduli spaces of structures on curves that degenerate at a finite set of points. Branched covers are the first obvious example, but if we increase the dimension of the fibre by one, we can consider moduli spaces of Lefschetz fibrations (surfaces mapping to curves, with finitely many nodal fibres). Here the algebraic geometry is much more difficult, and there is no proven stability theorem of any sort. Still, it would be nice to try to prove one, and to see what the result says about the occurrence of Lefschetz fibrations with specified nodes.

Yet another interesting project would be to examine what the corresponding number field question is. Certainly this has something to do with enumerating curves defined over a given number field, with data on the set of primes where the curve has bad reduction, but it would be nice to make this more concrete.

A.12 Wood, Melanie

I am interested in function field analogs of the Cohen Lenstra heuristics. I would like to learn more about the recent work of Ellenberg and Venkatesh. I am interested if class groups statistics for curves are affected by conditioning on geometric conditions on the curve.