Non-abelian Cohen-Lenstra Heuristics and Function Field Theorems

Notes by Tony Feng
for a talk by Melanie Wood

June 14, 2016

1 The Cohen-Lenstra Heuristics

Let K be an imaginary quadratic field. We know that Cl_K is a finite abelian group. The Cohen-Lenstra heuristics address the question: *as K varies, how often is Cl_K a particular group*?

Cohen-Lenstra ('84) predicted that for p odd

$$\mathrm{Prob}(\mathrm{Cl}_K[p^\infty] \cong G) = \frac{1}{\#\,\mathrm{Aut}(G)} \cdot \prod_{i \geq 1}(1 - p^{-i}).$$

This comes from the philosophy that, in the absence of "external" influences, objects should appear inversely proportional to their number of automorphisms. (This fails for $p = 2$, because we do know external influences from genus theory.)

This also predict *moments*. If A is an odd finite abelian group, then they predict

$$\mathbb{E}(\#\mathrm{Surj}(\mathrm{Cl}_K, A)) = 1.$$

This is called the "A-moment". It is a remarkable property of the Cohen-Lenstra distribution.

Remark 1.1. Why is this called a moment? If you take all homomorphisms instead of surjections, you get "mixed moments" of group invariants. We take surjections to get this nice answer.

There is a general probabilistic principle that *when moments don't grow too fast, they determine a unique distribution*.

However, it turns out that the A-moments grow too fast for any rigorous, quantitative measure of "don't grow too fast". The point is that the moments are really like homomorphisms (instead of surjections), which count the number of subgroups.

In this case, though, there are restrictions on the distribution such as that it must be supported on integers.

Theorem 1.2 (Wood '14)**.** *These moments determine a unique distribution on finite abelian groups.*

Moral. The moments are everything.

So from now on we'll focus on the moments.

2 The Davenport-Heilbronn Theorem

Class field theory tells us that

$$\mathrm{Cl}_K = \mathrm{Gal}(K^{\mathrm{unr,ab}}/K).$$

So a surjection $\mathrm{Cl}_K \twoheadrightarrow A$ has number-theoretic interpretation as an unramified A-extension of K. The A-moment is then counting the number of unramified A-extensions of K. This interpretation is the major way that counting results have been accessed.

Theorem 2.1 (Davenport-Heilbronn '71)**.** *We have*

$$\mathbb{E}(\#Surj(\mathrm{Cl}_K, \mathbb{Z}/3\mathbb{Z})) = 1.$$

The argument is by counting unramified $\mathbb{Z}/3$-extensions of quadratic fields, rather than working directly with ideal classes.

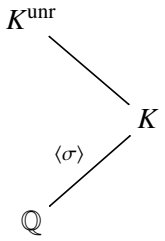
3 A non-abelian version

Let $G_K^{\mathrm{unr}} = \mathrm{Gal}(K^{\mathrm{unr}}, K)$. We can still ask about

$$\mathbb{E}(\#\mathrm{Surj}(G_K^{\mathrm{unr}}, H))$$

in other words the average number of unramified H-extensions of a K.

It turns out that there is a piece of structure here that was invisible in the abelian case.



We have an action of complex conjugation σ on G_K^{unr}. (In the abelianization σ acts by -1, so its presence is not felt in the abelian case.)

We can use group theory to reduce to studying

$$\mathbb{E}(\#\mathrm{Surj}_\sigma(G_K^{\mathrm{unr}}, H))$$

given H with an automorphism σ.

Boston, Bush, Hajir '14 gave heuristics for $G_K^{\mathrm{unr,pro}-p}$ (the Galois group of the maximal unramified pro-p extension of K, where p is odd). This group is often infinite (but can be finite). Here talking about probability is subtler, because we are a priori in the setting of uncountably many infinite pro-p groups. Impressively, they even gave empirical evidence for their heuristics.

In joint work with Nigel Boston, we reworked their heuristics in terms of a measure μ_{BBH} on the space of isomorphism classes of pro-p groups (in terms of an explicitly defined σ-algebra).

Proposition 3.1 (BW)**.** *When H is a finite p-group (p odd),*

$$\mu_{BBH}(H) = \frac{1}{\#\operatorname{Aut}_\sigma(H)} \cdot C.$$

This is a variant of the Cohen-Lenstra heuristics: objects should appear with probability inversely proportional to the number of automorphisms respecting all extra structure.

Proposition 3.2 (BW)**.** *Let H be a finite p-group and $\sigma \in \operatorname{Aut}(H)$ generator-inverting. Then*

$$\mathbb{E}(\#Surj_\sigma(\mu_{BHH}\ group, H)) = 1$$

and these moments determine μ_{BBH} uniquely.

4 Function Field Analogues

Replace $\mathbb{Q}$ with $\mathbb{F}_q(t)$. The analogue of an imaginary quadratic extension $K/\mathbb{F}_q(t)$ is a quadratic extension ramified at ∞.

Replace $\operatorname{Gal}(K^{\mathrm{unr}}/K)$ with $\operatorname{Gal}(K^{\mathrm{unr},\infty}, K)$, the Galois group of the maximal everywhere-unramified extension of K which is split completely at ∞. In particular, the abelianization of $\operatorname{Gal}(K^{\mathrm{unr},\infty}, K)$ is the affine class group (whereas the abelianization of $\operatorname{Gal}(K^{\mathrm{unr}}/K)$ contains the constant field extensions).

Theorem 4.1. *Let H be an odd finite group and σ be a generator-inverting automorphism of H, and $Z(H)^\sigma = 1$. Then*

$$\lim_{q\to\infty} \mathbb{E}^{\sup\,/\,\inf}(\#Surj_\sigma(\operatorname{Gal}(K^{\mathrm{unr},\infty}/K), H)) = 1$$

where the limit runs through q such that $(q, 2|H|) = 1$ (ruling out wild inertia) and $(q - 1, |H|) = 1$ (so there are no extra roots of unity).

Remark 4.2. In this theorem first q is fixed and the discriminant of K goes to ∞, and then q goes to infinity. We expect the result to be true without the q limit, but this is the best we can prove.

5 Remarks on the proof

The proof is in the direction of work of Ellenberg, Venkatesh, Westerland ('09) when H is *abelian* (that is the main result of the paper).

The idea is to consider Hurwitz spaces that parametrize extensions of $\mathbb{P}^1$, and count $\mathbb{F}_q$-points on them using Grothendieck-Lefschetz. Finally, use topology to bound the Betti numbers.

The necessity of taking the limit $q \to \infty$ is that there can be unstable cohomology which we cannot control.