A geometric approach to the Cohen-Lenstra heuristics

Aaron Landesman

It is well known to experts that moduli spaces exist whose integer points parameterize n-torsion elements in class groups of quadratic number fields. In particular, counting points of bounded height on these spaces is tantamount to solving cases of the Cohen-Lenstra heuristics. We explain why many of these moduli spaces have the following relatively simple form: They are the quotient of the complement of a hypersurface in affine space by the action of an algebraic group. We will also describe how this lets us view n-torsion in class groups of quadratic fields as n-Selmer groups of singular genus 1 curves.

This investigation is motivated by the Cohen-Lenstra heuristics, which describe the average number of n-torsion elements in class groups of quadratic number fields. It is an important open question in arithmetic statistics to count the asymptotic number of these n-torsion elements in quadratic fields.

A simple-to-state consequence of our approach is the following:

Theorem 1 Under the correspondence between quadratic forms and line bundles on spectra of rings of integers of quadratic fields, a quadratic form q corresponds to an n-torsion line bundle if and only if there exists a degree n homogeneous polynomial $f := \sum_{i=0}^{n} t_i x^i y^{n-i} \in \mathbb{Z}[x, y]$ whose resultant with q is ± 1, where the resultant is defined below in (1).

In fact, our approach gives a more precise parameterization of n-torsion elements in quadratic fields, as detailed in [1, Theorem 1.3]. Namely, n-torsion elements in class groups of varying quadratic extensions of $\mathbb{Z}$ are in bijection with $\mathbb{Z}$ points of the quotient stack $[U/G]$, with U and G defined as follows. Consider the affine space $\mathbb{A}_{\mathbb{Z}}^{3+(n+1)}$ parameterizing the coefficients $(a, b, c), (t_0, \dots, t_n)$, where a, b, c are the coefficients of a quadratic form $q := ax^2 + bxy + cy^2$ and t_i are the coefficients of a degree n binary form $f := \sum_{i=0}^{n} t_i x^i y^{n-i}$. Then, define U as the complement of the hypersurface $\mathrm{Res}(q, f) = 0$, where $\mathrm{Res}(q, f)$ denotes the resultant given as the determinant of the matrix

$$\mathrm{Res}(q, f) := \begin{pmatrix} a & 0 & \cdots & 0 & t_0 & 0 \\ b & a & \cdots & 0 & t_1 & t_0 \\ c & b & \ddots & 0 & t_2 & t_1 \\ \vdots & \vdots & \ddots & 0 & \vdots & \vdots \\ 0 & 0 & \ddots & 0 & t_{n-2} & t_{n-3} \\ 0 & 0 & \ddots & a & t_{n-1} & t_{n-2} \\ 0 & 0 & \ddots & b & t_n & t_{n-1} \\ 0 & 0 & \cdots & c & 0 & t_n \end{pmatrix}. \tag{1}$$

The group G is most naturally realized as the automorphism group of the Hirzebruch surface $\mathrm{Proj}_{\mathbb{P}^1}(\mathcal{O}_{\mathbb{P}^1}(2) \oplus \mathcal{O}_{\mathbb{P}^1}(n))$. It can also be explicitly described as generated by the actions of $\mathbb{G}_m, \mathrm{GL}_2, \mathbb{G}_a^{n-1}$, where $\lambda \in \mathbb{G}_m$ acts by sending $(q, f) \mapsto (\lambda q, \lambda f)$, $g \in \mathrm{GL}_2$ acts by sending $(q(x,y), f(x,y)) \mapsto \frac{1}{\det(g)} \cdot (q(gx, gy), f(gx, gy))$ and $(\alpha_0, \ldots, \alpha_{n-2}) \in \mathbb{G}_a^{n-1}$ sends $(q, f) \mapsto (q, f + \sum_{i=0}^{n-2} \alpha_i x^i y^{n-2-i} q)$.

It turns out there is a nearly equivalent description of the above quotient stack, which we describe next. Let S denote the secant variety to the rational normal curve in $\mathbb{P}^n$, and let $W \subset S$ denote the open subscheme where one removes the rational normal curve. Then, then $[U/G]$ can be identified with $[W/\mathrm{PGL}_2]$, acting as automorphisms of the rational normal curve, see [2, Proposition 6.1.1].

Given the above relatively simple moduli spaces, it is natural to ask whether there is any way to use them to count n-torsion elements in class groups of quadratic fields.

Question 2 Is it possible to use these moduli spaces to obtain bounds on the asymptotic number of n-torsion elements in class groups of quadratic fields?

The above moduli spaces are in fact closely connected to Selmer groups of certain singular genus 1 curves, or equivalently Selmer groups of tori which are the smooth locus of these singular genus 1 curves. More precisely, suppose we start with a degree 2 cover $g : \mathrm{Spec}\, \mathcal{O}_K \to \mathrm{Spec}\, \mathbb{Z}$. One can then relate $\mathrm{Cl}(\mathcal{O}_K)[n]$ to the n-Selmer group of the relative dimension 1 torus $g_* \mathbb{G}_m / \mathbb{G}_m$ as in [1, Lemma 10.2].

Example 3 In the case that $n = 3$, the moduli space $[U/G]$ described above parameterizes G-orbits of pairs (q, f) where $q = ax^2 + bxy + cy^2$ and $f = t_0 x^3 + t_1 x^2 y + t_2 xy^2 + t_3 y^3$. Associated to this, one can form the singular genus 1 curve given as the vanishing locus of $zq + f = z(ax^2 + bxy + cy^2) + (t_0 x^3 + t_1 x^2 y + t_2 xy^2 + t_3 y^3)$ in $\mathbb{P}^2_{[x,y,z]}$. This is singular at at the point $x = y = 0$. By chasing various cohomological exact sequences as in [1, Lemma 10.2], one can relate the n-Selmer group of the relative Jacobian of this genus 1 curve to the n-torsion in the class group of the quadratic extension whose discriminant is $b^2 - 4ac$.

The above observation that class groups of quadratic fields can be described in terms of Selmer groups of 1-dimensional tori suggests the following question.

Question 4 Can one create a unified set of heuristics which govern n-Selmer groups of (not necessarily proper) algebraic groups that also imply the Cohen-Lenstra-Martinet heuristics for class groups of number fields?

References

[1] A. Landesman, *A geometric approach to the Cohen-Lenstra heuristics*, https://arxiv.org/abs/2106.10357v1, (2021).

[2] A. Landesman, *A thesis of minimal degree: two*, Thesis (Ph.D.)–Stanford University, (2021).