Heuristics on p-class towers of imaginary quadratic fields

Farshid Hajir
(joint work with Nigel Boston, Michael R. Bush)

Fix an odd prime p. For a number field K, let A_K be the p-Sylow subgroup of the ideal class group of K. Cohen and Lenstra [2] studied the frequency with which a given p-group occurs as A_K where K ranges over all imaginary quadratic fields, ordered according to the absolute value of discriminant. They showed that there is a probability measure on p-groups of fixed p-rank in which the measure of each group is inversely proportional to the size of its automorphism group. Positing that this measure is the frequency with which G occurs as A_K, they arrived at the following conjecture.

Conjecture 1 (Cohen-Lenstra)**.** *For a fixed positive integer g, among the imaginary quadratic fields K such that the p-rank of A_K is g, ordered by discriminant, the probability that A_K is isomorphic to $G = \mathbb{Z}/p^{r_1} \times \cdots \times \mathbb{Z}/p^{r_g}$ is*

$$\frac{1}{|\operatorname{Aut}(G)|} \cdot \frac{1}{p^{g^2}} \prod_{k=1}^{g} (p^g - p^{g-k})^2.$$

We extend the Cohen-Lenstra heuristic to a non-abelian setting by considering, for each imaginary quadratic field K, the pro-p fundamental group G_K of the ring of integers of K. Concretely, G_K is the Galois group of the p-class tower of K, i.e. $G_K := \operatorname{Gal}(K_\infty/K)$ where K_∞ is the maximal unramified p-extension of K. Note that, by class field theory, A_K is isomorphic to G_K^{ab}, the maximal abelian quotient of G_K.

Put $d(G) = \dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p), r(G) = \dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p)$ for the minimal number of generators and relations of a pro-p group G, respectively. Though the group G_K is rather mysterious for general number fields K, for imaginary quadratic K, it satisfies certain restrictive conditions, namely G_K is a Schur σ-group, in the terminology of Koch and Venkov [3]. We recall that a finitely generated pro-p group G is called a Schur σ-group of rank g if it satisfies the following properties: 1) $d(G) = r(G) = g$; 2) G^{ab} is finite; 3) There exists an element $\sigma \in \operatorname{Aut}(G)$ of order 2 acting as inversion on G^{ab}.

We establish that there is a natural Cohen-Lenstra measure in the category of Schur σ-groups. Our main heuristic assumption then is that for the sequence of p-class tower groups of imaginary quadratic fields, ordered by discriminant, or more generally for the sequence of maximal p-class c quotients of these p-class tower groups (where c is any fixed whole number), the frequency of any given group equals the measure of the group in a corresponding category of Schur σ-groups. Our main group-theoretical result is a computation of this measure, which then leads to the following conjecture.

Conjecture 2. *Suppose G is a finite p-group which is a Schur σ-group of generator rank $g \geq 1$ or, more generally, suppose c is a positive integer and G is the maximal p-class c quotient of a Schur σ-group of rank g. Then, among the imaginary*

quadratic fields K such that A_K has rank g, ordered by discriminant, the probability that G_K (or in the fixed p-class case, the maximal p-class c quotient of G_K) is isomorphic to G is equal to

$$\frac{z(G)^g}{|\operatorname{Aut}(G)|} \cdot \frac{1}{p^{gh}} \prod_{k=1}^{g} (p^g - p^{g-k}) \prod_{k=1}^{h} (p^g - p^{h-k}),$$

where h is the difference between the p-multiplicator rank and nuclear rank of G (so $0 \le h \le g$ with $h = g$ for Schur σ-groups) and $z(G)$ is the number of fixed points of an automorphism σ acting as inversion on the abelianization of G.

The quantity $z(G)$ is independent of the choice of order 2 automorphism σ acting as inversion on G^{ab}; moreover, the ratio $z(G)^g/|\operatorname{Aut}(G)|$ can also be written as $1/|\operatorname{Aut}_\sigma(G)|$ where $\operatorname{Aut}_\sigma(G)$ is the subgroup of automorphisms which commute with σ. Comparing the form of Conjectures 1 and 2, we note that in the case of G being a Schur σ-group, for which we have $h = g$, the two predicted frequencies differ only in that $\operatorname{Aut}(G)$ is replaced by $\operatorname{Aut}_\sigma(G)$. Note that for abelian groups G, we have $z(G) = 1$, hence the two formulae match and indeed, suitably interpreted, Conjecture 2 generalizes Conjecture 1.

The numerical study of Conjecture 2 presents some interesting challenges, even in the simplest case of $p = 3, g = 2$ to which we limited our computations. Note that we do not even know an algorithm for determining whether G_K is finite, much less for computing it, and few examples have actually been completely worked out. One of the first examples of a computation of G_K in the literature appears in a 1934 article of Scholz and Taussky [4]: for the field $\mathbb{Q}(\sqrt{-4027})$, with $p = 3$, A_K is elementary abelian of rank 2 and the group G_K, of size 243, is isomorphic to the group denoted `SmallGroup(243,5)` in the terminology of the computer algebra software package `Magma`[1] which we used for all of our computations.

In order to test our heuristic hypothesis, we considered what kind of number-theoretical data (meaning about the groups G_K) was within reach and settled on the following: we computed the class groups of unramified extensions of K of degree 1 or p. In terms of group theory, this "index $\le p$ abelianization data" or "IPAD," describes the abelianization of G_K as well as those of its index p subgroups. Though it is impractical at present to attempt the complete computation of G_K for all but a handful of fields K, it was possible for us to compute the IPADs of quite a few such p-class tower groups and to compare them to the group-theoretical prediction. Given the variability of the data and the general convergence trend toward the predicted value, we believe that, within the limitations of the computation, the data supports our conjecture. To cite one example, the group of largest measure among 3-groups which are Schur σ-groups of rank 2 is `SmallGroup(243,5)` and happens to be determined uniquely by its IPAD. Using our main theorem, we find its measure to be $128/729 \approx 0.1756$. For discriminants whose absolute values lie in the ranges $(0, 2 \cdot 10^5)$, $[2 \cdot 10^5, 4 \cdot 10^5)$, $[4 \cdot 10^5, 6 \cdot 10^5)$, $[6 \cdot 10^5, 8 \cdot 10^5)$, this group occurs as G_K with frequency approximately 21.07%, 21.87%, 17.50%, 17.27% for a cumulative total of 19.26%.

References

[1] W. Bosma, J. J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., **24** (1997), 235–265.
[2] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, pp. 33–62 in: Number theory, Noordwijkerhout 1983, LNM **1068**, Springer, Berlin, 1984.
[3] H. Koch and B.B. Venkov, *Über den p-Klassenkörperturm eines imaginär-quadratischen Zahlkörpers*, Soc. Math. France, Astérisque **24-25** (1975), 57–67.
[4] A. Scholz and O. Taussky, *Die Hauptideale der kubischen Klassenkörper imaginär-quadratischer Zahlkörper*, J. Reine Angew. Math. **171** (1934), 19–41.

Reporter: Michiel Kosters