Heuristics for $p$-class Towers of Imaginary Quadratic Fields

Nigel Boston, Michael R. Bush and Farshid Hajir

With An Appendix by Jonathan Blackhurst

Dedicated to Helmut Koch

Abstract

Cohen and Lenstra have given a heuristic which, for a fixed odd prime $p$, leads to many interesting predictions about the distribution of $p$-class groups of imaginary quadratic fields. We extend the Cohen-Lenstra heuristic to a non-abelian setting by considering, for each imaginary quadratic field $K$, the Galois group of the $p$-class tower of $K$, i.e. $G_K := \text{Gal}(K_\infty/K)$ where $K_\infty$ is the maximal unramified $p$-extension of $K$. By class field theory, the maximal abelian quotient of $G_K$ is isomorphic to the $p$-class group of $K$. For integers $c \geq 1$, we give a heuristic of Cohen-Lenstra type for the maximal $p$-class $c$ quotient of $G_K$ and thereby give a conjectural formula for how frequently a given $p$-group of $p$-class $c$ occurs in this manner. In particular, we predict that every finite Schur $\sigma$-group occurs as $G_K$ for infinitely many fields $K$. We present numerical data in support of these conjectures.

1. Introduction

1.1 Cohen-Lenstra Philosophy

About 30 years ago, Cohen and Lenstra [9, 10] launched a heuristic study of the distribution of class groups of number fields. To focus the discussion, we restrict to a specialized setting. Let $p$ be an odd prime. Among the numerous insights contained in the work of Cohen and Lenstra, let us single out two and draw a distinction between them: (1) There is a natural probability distribution on the category of finite abelian $p$-groups for which the measure of each $G$ is proportional to the reciprocal of the size of $\text{Aut}(G)$; and (2) the distribution of the $p$-part of class groups of imaginary quadratic fields is the same as the Cohen-Lenstra distribution of finite abelian $p$-groups. The first statement, a purely group-theoretic one, is quite accessible and, indeed, in the first part of [10], Cohen and Lenstra prove many beautiful facts about the distribution of more general modules (not just over $\mathbb{Z}$ but more generally over rings of integers of number fields). The second, and bolder, insight is much less accessible at present but leads to striking number-theoretic predictions, only a small number of which have been proven, but all of which agree with extensive numerical data. Note that (2) quantifies the notion that the (rather elementary) necessary conditions for a group to occur as the $p$-part of the class group

2010 Mathematics Subject Classification 11R29, 11R11

Keywords: Cohen-Lenstra heuristics, class field tower, ideal class group, Schur $\sigma$-group

The research of the first author is supported by NSA Grant MSN115460. The computations made use of a portion of Smith College’s math grid funded by NSF Grant DMS-0721661.
In the decades since the publication of [9, 10], the application of (1) has been broadened to a number of other situations. It should be noted, however, that there are many circumstances where the weighting factor should also involve some power of the order of $G$. This includes recent investigations into variation of Tate-Shafarevich groups, variation of $p$-class tower groups ($p$ odd) for real quadratic fields (to be described in a subsequent paper by the authors) and variation in presentations of $p$-groups as described in [5]. The case under consideration in the current paper, however, does not involve these extra factors.

As regards the combination of (1) and (2), one can speak of a “Cohen-Lenstra strategy,” perhaps, as follows. Suppose we have a sequence $G_1, G_2, \ldots$ of $p$-groups (arising as invariants attached to some kind of arithmetic objects, say). One can hope to identify a category $C$ of groups in which the sequence lies and to define a probability measure on that space for which the measure of each group $G$ is proportional to $\psi(|G|)/|\text{Aut}_C(G)|$, where $\psi$ is a suitable function and $\text{Aut}_C(G)$ is the set of automorphisms of $G$ in the category $C$. The Cohen-Lenstra philosophy then would say that, assuming the sequence $(G_n)_{n \geq 1}$ is sufficiently general and the category $C$ is correctly chosen, the frequency with which any object $G$ of $C$ occurs in the sequence $(G_n)_{n \geq 1}$, defined to be the limit

$$\lim_{n \to \infty} \frac{\sum_{\nu=1}^n \text{ch}_G(G_\nu)}{n},$$

assuming it exists, is just the same as the Cohen-Lenstra measure of $G$ in the category $C$. Here, $\text{ch}_G(H)$ is the characteristic function of $G$, taking the value 1 if $H$ is isomorphic to $G$ (in the category $C$) and 0 otherwise. In such a situation, we can speak of the sequence $(G_n)$ “obeying a Cohen-Lenstra distribution for the category $C$.”

As just some of the examples of applications of this philosophy we cite Cohen-Martinet [11], Wittman [22], and Boston-Ellenberg [6]. In the first two of these, the class groups are in fact studied as modules over the group ring of the Galois group. In [6], the groups under study are non-abelian, and in fact the situation is slightly different because the base field is fixed (to be $\mathbb{Q}$) and the ramifying set varies; however the essential Cohen-Lenstra idea appears to apply in that situation also.

1.2 Cohen-Lenstra for $p$-class tower groups

In this article, we consider a non-abelian extension of the number-theoretic objects studied by Cohen and Lenstra, passing from the $p$-part of the class group of an imaginary quadratic field $K$ (we continue to assume $p$ is odd) to the pro-$p$ fundamental group of the ring of integers of $K$, namely the Galois group of its maximal everywhere unramified $p$-extension. For brevity, henceforth we will refer to these groups as “$p$-class tower groups.” The key fact, as pointed out in Koch-Venkov [17], is that $p$-class tower groups (and certain of their quotients) must satisfy a “Schur $\sigma$” condition; the precise definitions are given below. We establish that there is a natural Cohen-Lenstra measure in the category of Schur $\sigma$-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 $\sigma$-groups.

To describe our situation in more detail, we specify some notation to be used throughout the paper. For a pro-$p$ group $G$, we write $d(G) = \dim_{\mathbb{Z}/p\mathbb{Z}} H^1(G, \mathbb{Z}/p\mathbb{Z})$ and $r(G) = \dim_{\mathbb{Z}/p\mathbb{Z}} H^2(G, \mathbb{Z}/p\mathbb{Z})$, \ldots
\]
Heuristics for $p$-class Towers of Imaginary Quadratic Fields

where the action of $G$ on $\mathbb{Z}/p\mathbb{Z}$ is trivial; these give, respectively, the generator rank and relation rank of $G$ as a pro-$p$ group. The Frattini subgroup of $G$, $\Phi(G)$, is defined to be the closure of $[G,G]G^p$. The groups $G^{ab} = G/[G,G]$ and $G/\Phi(G)$ are, respectively, the maximal abelian quotient and maximal exponent-$p$ abelian quotient of $G$.

For an imaginary quadratic field $K$, we let $A_K$ be the $p$-Sylow subgroup of the ideal class group of $K$. If we allow $K$ to vary over all imaginary quadratic fields, ordered according to increasing absolute value of the discriminant $d_K$, the groups $A_K$ fluctuate with no immediately apparent rhyme or reason, but regarding their cumulative behavior, Cohen and Lenstra asked what can be said about the frequency with which a given group would occur as $A_K$ for some $K$. Their heuristic, described above, led them to many predictions, one of which is the following conjecture.

**Conjecture 1.1 Cohen-Lenstra.** For a fixed positive integer $g$, among the imaginary quadratic fields $K$ such that $A_K$ has rank $g$, 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

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

**Remark 1.2.** Since this statement is not explicitly in the Cohen-Lenstra papers, let us point out how it follows immediately from their work. It is a theorem of Hall [16] and, in a more general context, of Cohen-Lenstra (Cor. 3.8 of [10]), that the sum of $1/|\text{Aut}(G)|$ as $G$ runs over all isomorphism classes of abelian $p$-groups is

$$\prod_{n \geq 1} (1 - p^{-n})^{-1}.$$ 

We also have, see p. 56 of [10], that the probability that an abelian $p$-group has generator rank $g$ is

$$p^{-g^2} \prod_{n \geq 1} (1 - p^{-n}) \prod_{k=1}^g (1 - p^{-k})^{-2}.$$ 

Thus, under the Cohen-Lenstra distribution, for a given abelian $p$-group $G$, the probability that an abelian $p$-group of generator rank $g$ is isomorphic to $G$ is given by the quantity in Conjecture 1.1. Cohen-Lenstra’s fundamental heuristic assumption then yields Conjecture 1.1.

To describe how we pass to a non-abelian generalization, recall that if $K_1$ is the $p$-Hilbert class field of $K$, defined to be its maximal abelian unramified $p$-extension, then there is a canonical isomorphism $A_K \to \text{Gal}(K_1/K)$ given by the Artin reciprocity map. Now, let us consider the field $K_\infty$ obtained by taking the compositum of all finite unramified $p$-extensions of $K$, not just the abelian ones. We put $G_K = \text{Gal}(K_\infty/K)$. It is clear that the maximal abelian quotient of $G_K$ is isomorphic to $A_K$ and by Burnside $d(G_K) = d(A_K)$.

The central question we consider in this work is: For a fixed odd prime $p$, as $K$ varies over all imaginary quadratic fields of ascending absolute value of discriminant, what can one say about the variation of the groups $G_K$?

Naturally, this is a more difficult question than the variation of class groups, even for venturing a guess. Already, the group $G_K$ is not always finite. Indeed, in [17], Koch and Venkov proved that $G_K$ is infinite if $d(G_K) \geq 3$; they did so by taking into account all the facts they had at their disposal about the group $G_K$. Namely, $G_K$ is a finitely generated pro-$p$ group with
finite abelianization and deficiency 0 (meaning that \( r(G_K) - d(G_K) = 0 \)) and admits an automorphism of order 2 which acts as inversion on its abelianization (complex conjugation is such an automorphism, for example). Since having zero deficiency is equivalent to having trivial Schur multiplier in this context, Koch and Venkov dubbed groups having this particular set of properties “Schur \( \sigma \)-groups.” In Section 2, we review some of the work of Koch and Venkov, introduce Schur \( \sigma \)-groups, and assign a Cohen-Lenstra type measure for Schur \( \sigma \)-groups and some of their quotients.

Insight (2) of Cohen and Lenstra was that the most fundamental restriction on the \( p \)-part of the class group, namely that it is a finite abelian \( p \)-group, appears to be the only restriction on it. In just the same way, positing our main heuristic assumption that a finite \( p \)-group \( G \) arises as a \( p \)-class tower group over an imaginary quadratic field with the same frequency as \( G \) occurs as a randomly chosen group among Schur \( \sigma \)-groups, in Section 3 we arrive at the following Conjecture, which should be compared to the Cohen-Lenstra Conjecture above.

**Conjecture 1.3.** Suppose \( G \) is a finite \( p \)-group which is a Schur \( \sigma \)-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 \( \sigma \)-group. 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

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

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

**Remark 1.4.** We note that the quantity \( z(G) \) is independent of the choice of \( \sigma \). For more details about this and other quantities that appear in the conjecture we refer the reader to Section 2. Comparing the form of Conjectures 1.1 and 1.3, we note that in the case of \( G \) being a Schur \( \sigma \)-group, the two predicted frequencies differ only by a factor of \( z(G)^g \); we give an explanation for this factor in Theorem 2.11. Note that for abelian groups \( G \), we have \( z(G) = 1 \), hence the two formulae match and indeed, suitably interpreted, Conjecture 1.3 generalizes Conjecture 1.1.

### 1.3 Numerical Evidence

As theoretical evidence for their conjecture, Cohen and Lenstra were able to show that a relatively cheap consequence of their heuristic assumption, namely the prediction that the average value of \( 3^{d_3(A_K)} \) (as \( K \) ranges over all imaginary quadratic fields) is 2, is in fact a highly non-trivial theorem of Davenport and Heilbronn [12]. In more recent work, for example see [2], Bhargava and his students have obtained deep refinements and extensions of the Davenport-Heilbronn result, in particular verifying further consequences of the Cohen-Lenstra and Cohen-Martinet conjectures.

As regards numerical evidence, class groups of imaginary quadratic fields can be computed via an efficient algorithm, and so the class group computations available to Cohen and Lenstra were quite extensive. In [10], they derived many consequences of their heuristic, every one of which matched and in some cases even “explained” the observed variation of the \( p \)-part of the class group of imaginary quadratic fields.

In our non-abelian situation, 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, so the numerical investigation of our heuristic is bound to be more tricky. One of the first examples of a computation of $G_K$ in the literature appears in a 1934 article of Scholz and Taussky [20]: for the field $\mathbb{Q}(\sqrt{-4027})$, with $p = 3$, $A_K$ is elementary abelian of rank 2 and the group $G_K$ has size 243 and is isomorphic to the group denoted $\text{SmallGroup}(243,5)$ in the terminology of the computer algebra software package Magma. The method of Boston and Leedham-Green [7] can be used for certain $K$ to produce a short list of candidates for the isomorphism class of $G_K$.

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 $\leq p$ 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. As summary of the numerical evidence, the last two columns of Table 2 in Section 5 list the observed and predicted frequencies of the most common IPADs. 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.

1.4 Organization of the paper

As in [10], we have separated the group theory, where we have theorems, from the number theory, where we mostly make conjectures and collect data. We develop some basic facts about Schur $\sigma$-groups in Section 2 and give a precise formulation of our conjecture describing the variation of Galois groups of $p$-towers of imaginary quadratic fields in Section 3. The distribution of IPADs of Schur $\sigma$-groups is investigated in Section 4. This investigation yields a number of results which we prove using a mixture of theory and computation, thanks to the powerful technique of organizing $p$-groups via O’Brien’s $p$-group generation algorithm [19]. Finally, the number-theoretical data we have collected is summarized in Section 5. All of the computations were done using the symbolic algebra package Magma [3].

2. Schur $\sigma$-groups

We fix an odd prime $p$. As indicated in the introduction, we are interested in the following family of groups.

Definition 2.1. A finitely generated pro-$p$ group $G$ is called a Schur $\sigma$-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 $\sigma \in \text{Aut}(G)$ of order 2 acting as inversion on $G^{ab}$.

We will also want to consider certain special finite quotients of these groups, namely their maximal quotients of a fixed $p$-class. To define this, let $P_0(G) = G$ and, for $n \geq 0$, $P_{n+1}(G)$ denote the (closed) subgroup generated by $[G, P_n(G)]$ and $P_n(G)^p$. The groups $P_0(G) \supseteq P_1(G) \supseteq P_2(G) \supseteq \ldots$ form a descending chain of characteristic subgroups of $G$ called the lower $p$-central series. Note that $P_1(G)$ is the Frattini subgroup $\Phi(G)$. The $p$-class $c$ of a finite $p$-group $G$ is the smallest $n \geq 0$ for which $P_n(G) = \{1\}$. If $N$ is a normal subgroup of $G$, and $G/N$ has $p$-class $n$, then $P_n(G) \leq N$. Thus, if $G$ has $p$-class $c$, then for $n = 0, \ldots, c$, the maximal $p$-class $n$ quotient of $G$ is $G/P_n(G)$. It will be important for us to give much consideration to the maximal $p$-class $n$ quotients of Schur $\sigma$-groups so we make the following definition.
Definition 2.2. Let $G$ be a finite $p$-group of $p$-class $c$. We say that $G$ is Schur (or Schur of $p$-class $c$) if it is the maximal $p$-class $c$ quotient of a Schur $\sigma$-group.

Suppose $G$ has $p$-class $c$. A pro-$p$ group $H$ satisfying $H/P_c(H) \cong G$ is called a descendant of $G$ and if, additionally, $H$ has $p$-class $c+1$, then $H$ is called a child, or immediate descendant, of $G$. O’Brien [19] produced an algorithm that computes all children (and so ultimately all descendants) of a given $p$-group. He also highlighted the importance of two invariants of a $p$-group $G$ for his algorithm, namely its $p$-multiplier rank and its nuclear rank. The first minus the second is always nonnegative and does not exceed $r(H)$ for any descendant $H$ of $G$ (Prop. 2 of [8]). If a group has nuclear rank 0, then it has no children and is called terminal. A Schur group of $p$-class $c$ which is terminal has no proper descendants but must be $H/P_c(H)$ for some Schur $\sigma$-group $H$; hence it is a Schur $\sigma$-group. Thus, terminal Schur groups are always Schur $\sigma$-groups. In the other direction, in the appendix (where basic definitions and facts about the $p$-multiplier and nucleus are provided), Blackhurst proves that a pro-$p$ group with trivial Schur multiplier must be terminal; this is a result to which several authors have referred, but there appears to be no proof in the literature. Since Schur $\sigma$-groups satisfy $r(G) = d(G)$, they have trivial Schur multiplier, hence finite Schur $\sigma$-groups are terminal. In summary, terminal Schur groups are the same as finite Schur $\sigma$-groups.

Suppose $G$ is Schur of $p$-class $c$ so that $G = H/P_c(H)$ for some Schur $\sigma$-group $H$. A choice of order 2 element $\sigma \in \text{Aut}(H)$ which acts as inversion on $H^\text{ab}$ induces an involution on $G$, (which, by abuse of notation, we will also call $\sigma$) because the subgroup $P_c(H)$ is a characteristic subgroup of $H$. Moreover, this automorphism of $G$ acts as inversion on $G^\text{ab}$. Thus, a Schur group $G$ is a Schur $\sigma$-group if and only if $r(G) = d(G)$. Using refinements of the theorem of Golod and Shafarevich, Koch and Venkov showed [17] that Schur $\sigma$-groups of rank at least 3 are always infinite. Much of our work will therefore focus on the case of rank 2 finite Schur $\sigma$-groups.

We now fix $g \geq 1$, and let $F$ denote the free pro-$p$ group on $g$ generators $x_1, \ldots, x_g$. Let $\sigma$ be the automorphism of $F$ induced by the assignment $\sigma(x_i) = x_i^{-1}$ for $i = 1, \ldots, g$. Koch and Venkov showed that the relations of a Schur $\sigma$-group can always be chosen to lie in

$$X = \{ t^{-1}\sigma(t) | t \in \Phi(F) \}.$$

This is a subset of

$$X' = \{ s \in \Phi(F) | \sigma(s) = s^{-1} \},$$

and in fact these two sets coincide, as we will see in a moment. First, just a bit more notation; for each positive integer $c$, we define

$$X_c = \{ t^{-1}\sigma(t) | t \in \Phi(F/P_c(F)) \}, \quad X'_c = \{ s \in \Phi(F/P_c(F)) | \sigma(s) = s^{-1} \}.$$

Lemma 2.3. With notation as above, we have $X = X'$ and $X_c = X'_c$ for all $c \geq 1$.

Proof. First, note that $\sigma(t^{-1}\sigma(t)) = \sigma(t)^{-1}t$ and so $X \subseteq X'$.

Second, note that $X$ is closed since it is the image of a compact set under a continuous map and that $X'$ is closed since it is defined by equality of two continuous functions in a Hausdorff space.

Since both sets are closed, it is sufficient to show that $X_c = X'_c$ for all $c \geq 1$. Note that $X_c$ and $X'_c$ are finite sets. As above, we have $X_c \subseteq X'_c$. Define a map $X'_c \to X_c$ by $s \mapsto s^{-1}\sigma(s) = s^{-2}$. Since $p$ is odd, this is injective, which establishes that $X_c = X'_c$. □

The sets $\Phi(F)$ and $X$ are closed and hence measurable. Furthermore, given a Schur $\sigma$-group $G$ of rank $g$, we can consider the set of ordered $g$-tuples taken from $X$ such that the pro-$p$ group
presented by these elements is isomorphic to \( G \). Denote this set \( Y(G) \). It is a closed, and hence measurable, subset of \( X^9 \). We denote its relative measure, i.e. the measure of \( Y(G) \) divided by that of \( X^9 \), by \( \text{Meas}(G) \). This represents the proportion of ways in which Schur-type relations present \( G \).

We can perform this computation in a more effective way by considering Schur groups, not just Schur \( \sigma \)-groups. Namely, if \( G \) is Schur of \( p \)-class \( c \) and has generator rank \( g \), then we let \( Y_c(G) \) denote the set of ordered \( g \)-tuples taken from \( X_c \) that present \( G \) as a quotient of \( F/P_c(F) \) and define \( \text{Meas}(G) \) to be the measure of \( Y_c(G) \) divided by that of \( X^9_c \). Note that the definition of \( \text{Meas}(G) \) for Schur groups of \( p \)-class \( c \) is more general but is consistent with the definition for Schur \( \sigma \)-groups. Moreover, as a result, we have given a finite algorithm for computing \( \text{Meas}(G) \) and exhibited this quantity as a rational number.

**Example 2.4.** As an example, let \( p = 3 \) and consider the finite 2-generated 3-groups of 3-class 2. O’Brien’s algorithm yields 7 such groups, of which 3 are Schur. In this case \( F/P_2(F) \) has order \( 3^5 \) and we calculate that the set \( X_2 \) is an elementary abelian subgroup of order 9. Of these 3 Schur groups, the one of order 27 - call it \( G_1 \) - arises when the ordered 2-tuple taken from \( X_2 \) generates \( X_2 \). This happens for 48 of the 81 ordered 2-tuples. Thus \( \text{Meas}(G_1) = 16/27 \).

The second group, of order 81 - call it \( G_2 \) - arises when the ordered 2-tuple generates one of the 4 subgroups of \( X_2 \) of order 3. Each of these 4 subgroups is generated by 8 of the 81 ordered 2-tuples in \( X_2 \times X_2 \); hence, \( \text{Meas}(G_2) = 32/81 \).

The third group, of order 243 - call it \( G_3 \) - is \( F/P_2(F) \) itself and arises when both entries in the 2-tuple are trivial. Therefore, \( \text{Meas}(G_3) = 1/81 \).

**Remark 2.5.** Note that there are two other 2-generated 3-groups of 3-class 2 that have a generator-inverting automorphism, namely \( \mathbb{Z}/3 \times \mathbb{Z}/9 \) and \( \mathbb{Z}/9 \times \mathbb{Z}/9 \). These groups arise as quotients of Schur \( \sigma \)-groups (indeed all the groups above are quotients of \( G_3 \)) but not as \( G/P_2(G) \) for any Schur \( \sigma \)-group \( G \) and so are not Schur groups.

These groups even have the difference between their \( p \)-multiplicator rank and nuclear rank equal to 2 and so are hard to distinguish from Schur groups. We refer to such groups as pseudo-Schur. These arise elsewhere, although rarely since in the situations we are considering, all the children of a group typically have the same order and so one cannot be a proper quotient of another. As an example, \( J_{22} \), introduced below in Section 4, has 2 Schur and 2 pseudo-Schur children, which are quotients of one of the Schur children by subgroups of order 3 fixed by the Schur automorphism.

**Remark 2.6.** In the above example, \( X_c \) happened to be a subgroup; in general, \( X \) and \( X_c \) are not subgroups but we can still obtain explicit formulae for \( \text{Meas}(G) \).

**Definition 2.7.** Suppose \( G \) is a Schur group of generator rank \( g \) and \( p \)-class \( c \). We let \( h(G) \) be the relation rank of \( G \) in the category of rank \( g \), \( p \)-class \( c \) Schur groups. This quantity satisfies \( 0 \leq h(G) \leq g \) and is the amount by which the multiplicator rank of \( G \) exceeds the nuclear rank of \( G \). If \( G \) happens to be a Schur \( \sigma \)-group, then \( h = g \) is also the relation rank of \( G \) in the category of pro-\( p \) groups. We define \( z(G) \) to be the number of fixed points of an automorphism \( \sigma \) of \( G \) which acts as inversion on its maximal abelian quotient. This quantity depends only on the group \( G \), not on the choice of automorphism \( \sigma \).

**Remark 2.8.** The reason \( z(G) \) depends only on \( G \) is that, as shown by Hall (section 1.3 of [15]), although sometimes attributed to Burnside, the kernel from \( \text{Aut}(G) \to \text{Aut}(G/\Phi(G)) \) is a pro-\( p \)
group and so by Schur-Zassenhaus (e.g. Prop. 1.1 of [14]), all lifts of order 2 of the inversion automorphism on \( G/\Phi(G) \) are conjugate to each other.

**Theorem 2.9.** Let \( G \) be Schur of rank \( g \) and put \( h = h(G) \). Then

\[
\text{Meas}(G) = \frac{z(G)^g}{|\text{Aut}(G)|} \cdot \frac{1}{p^{gh}} \prod_{k=1}^{g} (p^g - p^{g-k}) \prod_{k=1}^{h} (p^g - p^{h-k}).
\]

**Proof.** We compute the proportion of \( g \)-tuples of relators in \( \Phi(F) \) that present \( G \) following the strategy in [5], and then modify this to obtain \( \text{Meas}(G) \). First we count the number of epimorphisms from \( F \) to \( G \). Then we use this to count the number of normal subgroups \( R \) in \( F \) such that \( F/R \cong G \).

For a finite group \( \Gamma \), let \( \text{Epi}(F,\Gamma) \) be the set of epimorphisms from \( F \) to \( \Gamma \). Epimorphisms from \( F \) to \( \Gamma \) are in one-to-one correspondence with ordered \( g \)-tuples of elements of \( \Gamma \) that generate \( \Gamma \). There are \( |\Gamma|^g \) homomorphisms from \( F \) to \( \Gamma \) since the image of each generator is arbitrary. Since \( G \) is a \( p \)-group, by Burnside’s basis theorem the proportion of ordered \( g \)-tuples of elements of \( G \) that generate \( G \) equals the proportion of ordered \( g \)-tuples of \( G/\Phi(G) \) that generate \( G/\Phi(G) \cong (\mathbb{Z}/p)^g \).

There are \((p^g - p^{g-1})(p^g - p^{g-2}) \ldots (p^g - 1)\) of the latter \( g \)-tuples. In other words,

\[
\frac{\text{Epi}(F,G)}{|G|^g} = \frac{\text{Epi}(F,G/\Phi(G))}{|G/\Phi(G)|^g} = \frac{(p^g - p^{g-1})(p^g - p^{g-2}) \ldots (p^g - 1)}{|G/\Phi(G)|^g}.
\]

Thus, the number of ordered \( g \)-tuples of elements of \( G \) generating \( G \) is

\[
|\text{Epi}(F,G)| = |\Phi(G)|^g \cdot (p^g - p^{g-1})(p^g - p^{g-2}) \ldots (p^g - 1).
\]

Two epimorphisms have the same kernel if and only if they differ by an automorphism of \( G \), so dividing by \( |\text{Aut}(G)| \) gives the number of (closed) normal subgroups \( R \) of \( F \) with quotient isomorphic to \( G \).

Let \( c \) be the \( p \)-class of \( G \). A \( g \)-tuple of elements of \( R \) generate \( R \) as a normal subgroup if and only if their images generate \( R \) by the closed subgroup generated by \( [R,F], R^\sigma \), and \( P_c(F) \). This is an \( h \)-dimensional vector space \( V \) over \( \mathbb{F}_p \). The number of ordered \( g \)-tuples of vectors of \( V \) that generate \( V \) is \((p^g - p^{g-1})(p^g - p^{g-2}) \ldots (p^g - 1)\) and dividing by \( |V|^g = p^{gh} \) gives the proportion of them that generate \( V \). As \( \Phi(G) \cong \Phi(F)/R \), dividing by \( |\Phi(G)|^g \) gives the proportion of \( g \)-tuples in \( \Phi(F) \) that generate \( R \). Multiplying by the number of possible subgroups \( R \) we see that the proportion of \( g \)-tuples in \( \Phi(F) \) that present \( G \) is

\[
\frac{1}{|\text{Aut}(G)|} \cdot \frac{1}{p^{gh}} \prod_{k=1}^{g} (p^g - p^{g-k}) \prod_{k=1}^{h} (p^g - p^{h-k}).
\]
Heuristics for $p$-class Towers of Imaginary Quadratic Fields

forming a basis. Note that the action of $\sigma$ on this vector space is entirely inversion (by Koch-Venkov [17]). So if $a_1, \ldots, a_g$ lie in $A \cap R$, then their images in $R/R^n[F,R]$ are trivial and so the images of the $a_i t_i$, $i = 1, \ldots, g$ also form a basis and so generate $R$ as a normal subgroup.

It follows that for each of the cosets of $A^g$ containing a $g$-tuple presenting $G$, the total proportion of $g$-tuples in the coset with this property is $1/|A : A \cap R|^g = 1/|AR : R|^g = 1/z(G)^g$ since $AR/R \cong A(G) = \{g \in G | \sigma(g) = g\}$. It follows that $\text{Meas}(G)$, which can be viewed as the proportion of cosets of $A^g$ in $\Phi(F)^g$ containing a $g$-tuple presenting $G$, is the quantity (1) above divided by $1/z(G)^g$.

We explore the smallest non-trivial case, that of $g = 2$, $p = 3$. Here the theorem gives the simple formula $\text{Meas}(G) = 48kz(G)^2/|\text{Aut}(G)|$, where $k$ is the proportion of ordered pairs of vectors that span an $h$-dimensional vector space over $\mathbb{F}_3$ and $h = h(G)$. Typically, $h$ will be 2 and so $k = 16/27$. If $h = 1$, then $k = 8/9$. If $h = 0$, then $k = 1$.

We can check the formulae for $G_1, G_2, G_3$: we have $z(G_i) = 3$ for all $i$, $h(G_i) = 2, 1, 0$ respectively, and $|\text{Aut}(G_i)| = 432, 972, 34992$ respectively. Thus, $\text{Meas}(G_1) = 48 \times 16/27 \times 3^2 \times 1/432 = 16/27$; $\text{Meas}(G_2) = 48 \times 8/9 \times 3^2 \times 1/972 = 32/81$; $\text{Meas}(G_3) = 48 \times 1 \times 3^2 \times 1/34992 = 1/81$; which agree with the direct computations made in the above example.

We produce a table of the first few levels of Schur descendants of $G_1$ and their measures in the figure on the following page.
We next see that the measure we have defined is the same as that produced by the Cohen-Lenstra philosophy.

**Definition 2.10.** Let \( G \) be Schur, with a choice of involution automorphism \( \sigma \). We denote by \( \text{Aut}_\sigma(G) \) the set of all automorphisms which commute with \( \sigma \).

**Theorem 2.11.** If \( G \) is Schur with order 2 automorphism \( \sigma \) acting as inversion on \( G^{ab} \), then \(|\text{Aut}_\sigma(G)| = |\text{Aut}(G)|/z(G)^g|\).

**Proof.** We note that \( \text{Aut}_\sigma(G) \) is the centralizer of \( \sigma \) in \( \text{Aut}(G) \). Choose \( x_1, \ldots, x_g \in G \) that are inverted by \( \sigma \) and generate \( G \) (these exist by [4]). Then there is an injective map \( \text{Aut}(G) \to G^g \) given by

\[
\alpha \mapsto (\alpha(x_1), \ldots, \alpha(x_g)).
\]

Call its image \( V \). Let \( B = \{ x \in G | \sigma(x) = x^{-1} \} \). Then the image of \( \text{Aut}_\sigma(G) \) under the above map is \( V \cap B^g \).

Let \( A = \{ x \in G | \sigma(x) = x \} \), of order \( z(G) \). Consider the map \( G \to B \) given by \( x \mapsto x^{-1} \sigma(x) \), which the argument of Lemma 2.3 shows to be surjective. The fibers of the map are right cosets of \( A \). This identifies the image of \( \text{Aut}_\sigma(G) \) in \( G^g \) with \( A^g \setminus V \) and therefore its order equals \(|\text{Aut}(G)|/z(G)^g|\), as desired. \( \square \)

The theorem above implies that the conjugacy class of \( \sigma \) in \( \text{Aut}(G) \) has order \( z(G)^g \). It also implies the following corollary.

**Corollary 2.12.** The probability measure on the set of Schur \( \sigma \)-groups of rank \( g \) in which each such group \( G \) with involution \( \sigma \) has mass proportional to \( 1/|\text{Aut}_\sigma(G)| \) is the same as that given by \( \text{Meas}(G) \).

**Proof.** By Lemma 2.11, \( 1/|\text{Aut}_\sigma(G)| = z(G)^g/|\text{Aut}(G)| \), which by Theorem 2.9 is a constant multiplied by \( \text{Meas}(G) \) with the constant depending only on \( p \) and \( g \), which here are fixed. Finally, note that since probability measures have total mass 1, \( \text{Meas} \) is the only constant multiple of \( 1/|\text{Aut}_\sigma| \) that is a probability measure. \( \square \)

Every finite \( g \)-generated abelian \( p \)-group is a Schur \( \sigma \)-group in the category of abelian pro-\( p \) groups in the following sense: It has a generator-inverting automorphism of order 2, its abelianization is finite, and it has the same number of relations as generators. This last observation comes from the fact that if \( G \cong \mathbb{Z}/q_1 \times \ldots \times \mathbb{Z}/q_g \), then its relations in the category are \( x_i^{q_i} = 1 \), the commuting relations coming for free. Note further that \( z(G) = 1 \) since the automorphism fixes only the identity, or equivalently \( \text{Aut}_\sigma(G) = \text{Aut}(G) \). From this we see that the formula in Conjecture 1.3 is a direct generalization of the formula in Conjecture 1.1 and that abelian \( p \)-groups carry Schur \( \sigma \) structure “for free,” which is why this structure did not play an overt role in [9, 10].

There is also the following more direct connection between Conjecture 3.2 (a slightly stronger version of Conjecture 1.3 which applies to both finite and infinite Schur \( \sigma \)-groups) and Conjecture 1.1.

**Theorem 2.13.** Our measure, when pushed forward to the category of finite abelian \( p \)-groups of rank \( g \), is the Cohen-Lenstra measure. In particular, Conjecture 3.2 implies Conjecture 1.1.

**Proof.** The image of \( X \) under the natural projection from \( F \) to \( F^{ab} \) is \( \Phi(F^{ab}) \). This follows since if \( v \in \Phi(F^{ab}) \) then \( v = u^{-2} \) for some \( u \in \Phi(F^{ab}) \). Lifting \( u \) to \( x \in \Phi(F) \) and using the fact
that $\sigma$ restricts to the inversion automorphism on $F^{ab}$, we see that $x^{-1}\sigma(x) \in X$ lies in the preimage of $v$. Moreover, for each such $v$, the elements of the preimage can be put in one-to-one correspondence with the cosets of $F$ in $[F,F]$ where $F = \{x \in F \mid \sigma(x) = x\}$.

From this it follows that for any finite abelian $p$-group $C$, the proportion of sets of relations in $X^p$ which give rise to Schur $\sigma$-groups having fixed abelianization $C$ is equal to the proportion of sets of relations in $\Phi(F^{ab})^p$ giving rise to $C$ itself. The latter is exactly the quantity appearing in the Cohen-Lenstra distribution as demonstrated in [13].

\section{Conjectures}

In this section, we formulate our main heuristic assumption, then use the the group theory results of the previous section to make precise conjectures about the distribution of $p$-class tower groups of imaginary quadratic fields.

The arithmetic input, as already noted by Koch and Venkov, is three-fold. First, and most simply, we observe that for an imaginary quadratic field $K$, complex conjugation, whose restriction to $K$ generates $\text{Gal}(K/\mathbb{Q})$, has a natural action on arithmetic objects attached to $K$. In particular, since $\mathbb{Q}$ has trivial class group, $\mathbb{Q}$ is principal for every fractional ideal $a$ of $K$, so complex conjugation acts by inversion on $A_K$. More generally, complex conjugation acts as an involution on $G_K$, and as inversion on $G^{ab}_K \cong A_K$ thanks to the functorial properties of the Artin reciprocity map. The last two ingredients are the finiteness of the class group, and the vanishing of the $p$-rank of the unit group of $O_K$. The former ensures that $G_K$ has finite abelianization (as does every one of its open subgroups), and the latter that $r(G_K) = d(G_K)$, by a theorem of Shafarevich [21]. Thus, $G_K$ is always a Schur $\sigma$-group.

By its nature, the definition of the probability distribution we have imposed on Schur $\sigma$-groups puts the focus on finite Schur $\sigma$-groups; the latter only exist for generator rank at most 2. As we have seen, however, it is profitable to have a wider lens that captures not just Schur $\sigma$-groups but more generally the maximal $p$-class $c$ quotients of all pro-$p$ Schur $\sigma$-groups for $c \geq 1$.

**Definition 3.1.** For $x > 0$, let $F_x$ denote the set of imaginary quadratic fields with absolute value of discriminant not exceeding $x$, and for each natural number $g$, let $F_{x,g}$ be the subset of $F_x$ consisting of those fields $K$ having $d(A_K) = g$. For a finitely generated pro-$p$ group $G$, an imaginary quadratic field $K$, let $\text{ch}_G(G_K)$ be 1 if $G_K$ is isomorphic to $G$ and 0 otherwise. For a finitely generated pro-$p$ group $G$, let $g = d(G)$ be its generator rank, and define

$$\text{Freq}(G) = \lim_{x \to \infty} \frac{\sum_{K \in F_{x,g}} \text{ch}_G(G_K)}{\sum_{K \in F_{x,g}} 1}.$$

We can only conjecture that this limit exists; assuming that is so, $\text{Freq}(G)$ is the frequency with which $G$ occurs as a $p$-class tower group among the imaginary quadratic fields $K$ that have $d(A_K) = g$, which are the only ones that could have $G_K \cong G$.

More generally, if $G$ is a finite $p$-group, let $c$ be its $p$-class and $g$ its generator rank. We then define

$$\text{Freq}(G) = \lim_{x \to \infty} \frac{\sum_{K \in F_{x,g}} \text{ch}_G(G_K/P_c(G_K))}{\sum_{K \in F_{x,g}} 1},$$

assuming the limit exists. Note that if $G$ is terminal and so a Schur $\sigma$-group, then the two definitions coincide, so there is no ambiguity in the notation $\text{Freq}(G)$.
Heuristics for \( p \)-class Towers of Imaginary Quadratic Fields

Main Heuristic Assumption. For any fixed positive integer \( c \), the distribution of maximal \( p \)-class \( c \) quotients of \( p \)-class tower groups of imaginary quadratic fields ordered by increasing absolute value of discriminant obeys the Cohen-Lenstra distribution on Schur groups of \( p \)-class \( c \).

With the work of Section 2 under our belt, our Main Conjecture now flows from the above heuristic assumption.

Conjecture 3.2. For every pro-\( p \) group \( G \), we have

\[
\text{Freq}(G) = \text{Meas}(G).
\]

In particular, \( \text{Freq}(G) = 0 \) if \( G \) is not Schur. When \( G \) is finite and Schur, \( \text{Freq}(G) \) is given by the formula of Theorem 2.9 and stated as Conjecture 1.3 in Section 1.

In particular, as a consequence of Conjecture 3.2, we expect every finite Schur \( \sigma \)-group (respectively Schur \( p \)-group of \( p \)-class \( c \)) to occur as \( G_K \) (respectively \( G_K/P_c(G_K) \)) for a (positive proportion) of imaginary quadratic fields \( K \). It is worth noting that there are infinite Schur \( \sigma \)-groups that we do not expect to arise as \( G_K \) for any \( K \). For example, the Sylow 3-subgroup of \( SL_2(\mathbb{Z}_3) \) considered in [1] is a 2-generator 2-relator pro-3 group with finite abelianization and a generator-inverting automorphism, but the tame case of the Fontaine-Mazur conjecture implies that it does not arise as \( G_K \) for any \( K \). It is arbitrarily closely approximated by the finite Schur \( \sigma \)-groups in [1].

4. Index-\( p \)-Abelianization-Data (IPAD)

As discussed in the Introduction, complete calculation of \( G_K \) being prohibitive, we seek to put certain partial but accessible information about \( p \)-class tower groups under a general group-theoretical framework. Thus, in order to make comparisons with data coming from number theory it will be useful to consider abelianizations of low index subgroups. To that end we introduce the notion of IPAD. Thanks to the \( p \)-group generation algorithm, and the theory developed in Section 2, specializing to \( p = 3 \), we are able to prove precise measures for the most frequent IPADs, which we can then compare to the observed number-theoretical frequencies.

Definition 4.1. The abelian group \( \mathbb{Z}/q_1 \times \cdots \times \mathbb{Z}/q_d \) will be denoted \([q_1, \ldots, q_d]\). Given a \( g \)-generated pro-\( p \) group \( G \), its Index-\( p \) Abelianization Data (or IPAD for short) will be the unordered \((p^g - 1)/(p - 1)\)-tuple of abelianizations of the index \( p \) subgroups of \( G \) augmented by the abelianization of \( G \) itself; we always list the latter group first. It will be called IPAD(\( G \)).

For example, the IPAD of the Schur \( \sigma \)-group \texttt{SmallGroup}(243,5) will be denoted

\[[3,3]; [3,3,3][3,9]^3],

indicating that its abelianization is \([3,3]\) and those of its 4 index 3 subgroups are \([3,3,3]\), \([3,9]\), \([3,9]\), and \([3,9]\).

There are two things to note in working with IPADs [8]. First, considering \( g \)-generated pro-\( p \) groups for a fixed \( p \) and \( g \), if \( H \) is a quotient of \( G \), then each entry of IPAD(\( H \)) is a quotient of a corresponding entry of IPAD(\( G \)). This gives a partial order on IPADs and we say that IPAD(\( H \)) \( \leq \) IPAD(\( G \)). Second, if IPAD(\( G/P_n(G) \)) = IPAD(\( G/P_{n-1}(G) \)) (we call the IPAD settled), then IPAD(\( G \)) = IPAD(\( G/P_n(G) \)).
It follows that for a given IPAD there is a measurable subset of $X^g$ producing groups with that IPAD. We now compute, in the case $g = 2$ and $p = 3$, the measures of the most common IPADs.

**Theorem 4.2.** (1) IPAD $[[3,3];[3,3,3][3,9][3]]$ has measure $128/729 \approx 0.1756$;

(2) IPAD $[[3,9];[3,3,9][3,27][3]]$ has measure $256/2187 \approx 0.1171$;

(3) IPAD $[[3,3];[3,3,3][3,9]]$ has measure $64/729 \approx 0.0878$;

(4) IPAD $[[3,3];[3,3,3][3,9][3]]$ has measure $64/729 \approx 0.0878$;

(5) IPAD $[[3,3];[3,9][3,27][3]]$ has measure $512/6561 \approx 0.0780$;

(6) IPAD $[[3,3];[3,3,9][3,9][3]]$ has measure $512/6561 \approx 0.0780$;

(7) IPAD $[[3,3];[3,3,3][3,9][3]]$ has measure $2048/59049 \approx 0.0347$;

(8) IPAD $[[3,3];[3,3,3][3,9][3]]$ has measure $640/19683 \approx 0.0325$;

(9) IPAD $[[3,3];[3,9][3,27][3,3][3]]$ has measure $64/729 \approx 0.0878$;

(10) IPAD $[[3,3];[3,9][3,9]]$ has measure $16/729 \approx 0.0219$;

(11) IPAD $[[3,3];[3,9][3,27][3]]$ has measure $128/6561 \approx 0.0195$;

(12) IPAD $[[3,9];[3,3,9][3,9][3,9][3]]$ has measure $128/6561 \approx 0.0195$;

(13) IPAD $[[3,3,3][3,27][3,3][3]]$ has measure $64/729 \approx 0.0325$;

(14) IPAD $[[3,3,3][3,9][3,27][3,3][3]]$ has measure $64/729 \approx 0.0325$.

**Proof.** First, note that the abelianizations of $G_1, G_2, G_3$ are $[3, 3], [3, 9], [9, 9]$ respectively. It follows that any IPAD with first entry $[3, 3]$ has to come from descendants of $G_1$, and moreover that the first entry is settled, and so every descendant of $G_1$ has abelianization $[3, 3]$.

Thus, for all the cases above starting with $[3, 3], [3, 9]$ we focus on descendants of $G_1$. By O’Brien we compute that $G_1$ has 11 children. Of these, 7 have difference between $p$-multiplicator rank and nuclear rank at most 2 (in fact exactly 2) and all of these turn out to have a Schur automorphism. Call them $H_1, \ldots, H_7$ in the order produced by O’Brien’s algorithm as implemented in Magma

Of these, $H_3$ and $H_5$ are terminal and so are Schur $\sigma$-groups. In the standard database they are SmallGroup(243,5) and SmallGroup(243,7) respectively. Their IPADs are those on lines (1) and (4) above. We compute that $\text{Meas}(H_3) = 128/729$ and $\text{Meas}(H_5) = 64/729$. (1) and (4) follow by establishing that none of the Schur $\sigma$ descendants of the other $H_i$ have these IPADs. This also shows that these groups are determined by their IPADs.

Of the other IPADs, only $\text{IPAD}(H_4) \leq \text{IPAD}(H_3)$ (in fact equal). The Schur child of $H_4$ has IPAD including $[9, 9]$ and so does not contribute to (1). As for (4), we need to consider $H_1$, which has the same IPAD as $H_5$. Only one child of $H_1$, however, is Schur and its IPAD includes a $[9, 9]$ and so cannot contribute to (4). Thus, (1) and (4) are complete.

The Schur child of $H_1$ has 1602 children, of which 198 are Schur. All of these have $[3, 3][3, 3, 3][3, 9][27][2]$ as their IPAD and nuclear rank between 2 and 4. All the Schur children of 155 of these have the same IPAD, so are settled and they contribute 2048/59049 to line (8) above. The Schur children of the other 43 include $[27, 27]$, so do not count towards (8). The IPADs of the remaining $H_i$ are not less than or equal to this IPAD and so (8) is also complete.

The IPAD of $H_2$ is that on line (3) and all its children have the same IPAD. It therefore contributes $\text{Meas}(H_2) = 64/729$ to (3). None of the other $H_i$ has small enough IPAD that their descendants could have IPAD as in (3), and so (3) is proven.
The IPADs of $H_6$ and $H_7$ are both that given in line (10). All the children of $H_6$ have IPADs involving $[9,9]$, whereas the IPADs of all the children of $H_7$ are settled as (10). It follows that this IPAD has measure $\text{Meas}(H_7) = 16/729$, proving (10).

As for cases (5) and (6), these come from further investigation of descendants of $H_6$ and $H_4$ respectively. In each case, the group has a unique Schur child, which then has 6 Schur children. These all have the respective IPADs. In each case, 3 of the 6 are terminal, and the other 3 each have one Schur child. Two of those are settled, whereas the remaining group has larger IPAD. Thus 5 of the 6 Schur grandchildren of each $H_i$, whose measures are each $64/729$, contribute to (5) and (6) respectively and the remaining grandchild, whose measure is $64/6561$, does not. Thus the IPADs in (5) and (6) each have measure $64/729 - 64/6561 = 512/6561$, and (5) and (6) are proven.

IPADs (2), (7), (9), (11), (12), (13), and (14) above must come from descendants of $G_2$. This has 22 Schur children. We call these $J_1,\ldots,J_{22}$ in accordance with O’Brien’s ordering. Only $J_{10}, J_{11},$ and $J_{12}$ have IPADs less than or equal to (in fact equal to) that of (2). The last two are terminal and the unique Schur child of $J_{10}$ has larger IPAD. Thus, the IPAD of (2) has measure $\text{Meas}(J_{11}) + \text{Meas}(J_{12}) = 256/2187$, and (2) is proven.

The unique Schur child above has IPAD $[[3,9]; [3,3,9][3,9,9][3,27]^2]$. A Schur descendant of $G_2$ with IPAD in line (9) has to descend from this child (by comparing the IPADs of the other $J_i$). It has 9 Schur children, of which 6 have the IPAD of (9). The others have IPAD $[[3,9]; [3,3,9][9,9,9][3,27]^2]$, which is incomparable. Two of these are terminal, the other settled, and so this proves line (12). Of the remaining 6, there are 4 terminal groups, 1 settled, and 1 with a unique Schur child with larger IPAD. Summing the measures of the first 5 groups yields $640/19683$ and establishes (9).

Case (7) can only arise from descendants of $J_5$. It has 3 Schur children, with the 2 terminal ones having the desired IPAD and the other having larger IPAD. This establishes (7).

Case (11) arises from descendants of $J_{14}$ and $J_{17}$, all of which are settled, and so its measure is the sum of their measures. Case (13) similarly arises from $J_{13}$ and $J_{16}$, which are settled.

As for (14), this has to come from descendants of $J_{15}$ and $J_{18}$. Each has measure $64/6561$ and their trees of descendants are identical. Each has a unique Schur child and 4 Schur grandchildren. Of these, 1 is terminal and 2 others settled with the desired IPAD. The children of the remaining group have larger IPAD, so we subtract its measure, $64/59049$. Since $2(64/6561 - 64/59049) = 1024/59049$, (14) is proven.

Note that none of the 14 given IPADs have first entry greater than or equal to $[9,9]$ and so no descendants of $G_3$ will have one of these IPADs. Since the measure of $G_3$ is $1/81 = 0.0123$, the IPADs produced by its descendants will all have measure smaller than that of any of the 14 given IPADs.

The descendants of $H_1, H_4$, and $H_6$ appear to follow periodic patterns that lead to the following conjecture, which would complete the computation of measures of IPADs beginning $[3,3]$, since summing all their conjectured values gives $16/27 = \text{Meas}(G_1)$.

**Conjecture 4.3.** (a) If $k \geq 2$, then IPAD $[[3,3]; [3,9][3^k,3^{k+1}]]$ has measure $512/3^{2k+4}$;

(b) If $k \geq 2$, then IPAD $[[3,3]; [3,3,3][3,9][3^k,3^{k+1}]]$ has measure $512/3^{2k+4}$;

(c) If $k \geq 2$, then IPAD $[[3,3]; [3,3,3][3^k,3^{k+1}][3^{k+1},3^{k+2}]]$ has measure $2048/3^{4k+2}$;

(d) If $k \geq 2$, then IPAD $[[3,3]; [3,3,3][3^k,3^{k+1}][3^{k+1},3^{k+2}]]$ has measure $512/3^{4k+2}$.
Remark 4.4. 1. As noted, the measure of an IPAD is the sum of the measures of terminal and settled groups. If it only involves terminal groups, then it determines a finite list of groups having that IPAD. Sometimes, such as for lines (1) and (4) above, it determines a unique group. Now consider the IPAD in line (7), which corresponds to the two terminal Schur children of $J_5$. An imaginary quadratic number field with that IPAD (such as $\mathbb{Q}(\sqrt{-17399})$) therefore has one of these two groups as the Galois group of its 3-class tower, the first cases of a non-abelian 3-class tower of a quadratic field having 3-class length 4. This group has derived length 2. We have not found an IPAD consisting only of terminal groups of finite derived length exceeding 2.

2. In [17], Koch and Venkov proved that if a 2-generated Schur $\sigma$-group is finite, then it has relations at depth 3 and $k$ where $k \in \{3, 5, 7\}$ in the $p$-Zassenhaus filtration. McLeman [18] conjectures that the group is finite if and only if both relations have depth 3. Computing dimensions of the first three factors of the Jennings series, we observe that every Schur descendant of $G_1$ has its relations at this depth. The apparent combinatorial explosion in descendants of $H_1$ then casts doubt on the “if” part of McLeman’s conjecture.

As for Schur descendants of $G_2$, those not having both relations at depth 3 are precisely those descended from $J_6, \ldots, J_9, J_{19}, \ldots, J_{22}$. The combinatorial explosion in descendants of these groups lends support to the “only if” part of McLeman’s conjecture.

3. One might ask for the probability that a 2-generated Schur $\sigma$-3-group is finite. Searching through the tree, we find 90 descendants of $G_1$ that are Schur $\sigma$-groups of 3-class at most 11, 144 descendants of $G_2$ that are Schur $\sigma$-groups of 3-class at most 8, and 222 descendants of $G_3$ that are Schur $\sigma$-groups of 3-class at most 7. Their combined measure is slightly over $0.8533$ and so, in this sense, there is at least an $85.33\%$ probability that a 2-generated Schur $\sigma$-3-group is finite.

As for an upper bound, it is natural, in the spirit of Golod and Shafarevich, to conjecture that “large” IPADs will correspond only to infinite groups, but one must be careful. Extending the above census slightly, we find that $J_1$ has Schur $\sigma$-group descendants of 3-class 9 and order $3^{18}$ with IPAD $[3, 243]; [3, 3, 3, 81], [3, 729]^3$. Thus, having a rank 4 subgroup of index 3 (the highest rank possible by comparison with the free group) is not sufficient to imply that the Schur $\sigma$-group is infinite.

4. The $p$-class tower groups possess the FAb property, meaning that every open subgroup has finite abelianization. There do, however, exist Schur $\sigma$-groups that fail FAb, for example, the free pro-$p$ product $G$ of cyclic $p$-groups, which have finite $G/G'$ but infinite $G''/G'''$. Our conjecture indicates that the total measure carried by all non-FAb Schur $\sigma$-groups should be zero. Whilst we have not yet proven this, evidence for it is provided both by the fact that infinite abelian groups account for zero of the original Cohen-Lenstra measure and by the above conjecture, which indicates that groups with abelianization $[3, 3]$ and with an index 3 subgroup with infinite abelianization account for zero of our measure.

5. Computations

As evidence for our conjectures we have collected numerical data in the case of the smallest odd prime $p = 3$. For imaginary quadratic fields $K$ with 3-class group of rank 2 and discriminant $d_K$ satisfying $|d_K| < 10^6$ we have computed the 4 unramified cyclic extensions of degree 3 over $K$ and their 3-class groups. By class field theory, this yields the IPAD for the Galois group $G_K$.

Computations were carried out using the symbolic algebra package Magma [3] (Version 2.16) running on $12 \times 2.8$ GHz Quad-Core Intel Xeon processors running OS X Server 10.6.7. Each class group computation for an extension was carried out by a single Magma process assigned
Heuristics for $p$-class Towers of Imaginary Quadratic Fields

to one of the 48 available cores. The computations took place over a 10-month period although there were some short breaks when some or all of the cores were not in use.

Experimentation early on indicated a large amount of variation in the running times for the class group computations so the decision was made to set an arbitrary upper limit of 200 hours on each individual computation (although part way through the fifth interval of discriminants below this was increased to 300 hours). As a result, only partial IPAD data was obtained for 410 of the 3190 fields examined. For 189 of these, the IPAD computation was almost complete with 3-class group data for only one of the 4 extensions missing.

We now present a summary of the data collected. The first table is a census of the most common IPADs. The second lists their relative proportions obtained by dividing through by the total number of fields in the given interval, one obtains the proportions 0.6332, 0.2743, 0.0740 and 0.0107 respectively. Thus our IPAD census is automatically skewed towards those with smaller 3-class groups for this reason alone.

| I1  | I2  | I3  | I4  | I5  | Total |
|-----|-----|-----|-----|-----|-------|
| $[3, 3]; [3, 3, 3]$ | $[3, 3, 3]$ | $[3, 3, 3]^{3}$ | $[3, 9]$ | $[3, 27]$ | 597 |
| $[3, 3]; [3, 3, 3]$ | $[3, 3, 3]^{2}$ | $[3, 27]^{2}$ | $[3, 3, 3]^{4}$ | $[3, 9]$ | $[3, 27]$ | $[3, 9]^{2}$ | $[3, 9]$ | $[3, 27]$ | $[3, 9]^{3}$ | $[3, 27]^{3}$ | $[3, 9]^{4}$ | $[3, 27]^{4}$ | $[3, 81]^{2}$ | $[3, 9]^{5}$ | $[3, 27]^{5}$ | $[3, 9, 27]$ | $[3, 9, 27]^{2}$ | $[3, 27]^{2}$ | $[3, 9, 9, 9]$ | $[3, 9, 9, 9]^{2}$ | $[3, 9, 9, 9]^{3}$ | $[3, 9, 9, 9]^{4}$ | $[3, 9, 9, 9]^{5}$ | Other IPADs (49 types) | 3190 |
| 105 | 138 | 116 | 124 | 114 | 597 |
| 51  | 79  | 79  | 61  | 80  | 350 |
| 52  | 45  | 71  | 62  | 42  | 272 |
| 50  | 50  | 50  | 51  | 39  | 240 |
| 47  | 46  | 39  | 61  | 42  | 235 |
| 50  | 43  | 47  | 40  | 41  | 221 |
| 16  | 15  | 23  | 17  | 25  | 96  |
| 18  | 17  | 18  | 19  | 14  | 86  |
| 10  | 18  | 20  | 20  | 16  | 84  |
| 17  | 16  | 24  | 8   | 18  | 83  |
| 20  | 19  | 15  | 7   | 9   | 70  |
| 16  | 11  | 11  | 10  | 12  | 60  |
| 5   | 12  | 13  | 9   | 15  | 54  |
| 6   | 13  | 8   | 12  | 13  | 52  |
| 20  | 61  | 56  | 72  | 71  | 280 |
| 15  | 48  | 73  | 122 | 152 | 410 |
| Total | 498 | 631 | 663 | 695 | 703 | 3190 |

While there is certainly not exact agreement between the numerical and theoretical values, we still find this data promising. Given the relatively small size of the interval examined, one would not expect good convergence to the predicted limiting values. Indeed, if one takes a step back and simply examines the relative proportions of the four most common 3-class groups $[3, 3],[3, 9],[3, 27]$ and $[3, 81]$ for all fields in the given interval, one obtains the proportions 0.6332, 0.2743, 0.0740 and 0.0107 respectively. However the theoretical values predicted by the Cohen-Lenstra heuristics are 0.5926, 0.2634, 0.0878 and 0.0293 respectively. Thus our IPAD census is automatically skewed towards those with smaller 3-class groups for this reason alone.
| IPAD                          | $I_1$  | $I_2$  | $I_3$  | $I_4$  | $I_5$  | Cumulative | Predicted |
|-------------------------------|--------|--------|--------|--------|--------|------------|-----------|
| $[3, 3]; [3, 3, 3]$           | 0.2108 | 0.2187 | 0.1750 | 0.1622 | 0.1871 | 0.1756     |           |
| $[3, 9]; [3, 9, 3]$           | 0.1024 | 0.1252 | 0.1192 | 0.0878 | 0.1138 | 0.1097     | 0.1171    |
| $[3, 3]; [3, 3, 3]$           | 0.1044 | 0.0713 | 0.1071 | 0.0892 | 0.0597 | 0.0853     | 0.0878    |
| $[3, 3]; [3, 9, 27]$          | 0.1004 | 0.0792 | 0.0754 | 0.0734 | 0.0555 | 0.0752     | 0.0780    |
| $[3, 3]; [3, 3, 3]$           | 0.0944 | 0.0729 | 0.0588 | 0.0878 | 0.0597 | 0.0757     | 0.0878    |
| $[3, 3, 3]$; $[3, 9, 27]$     | 0.1004 | 0.0681 | 0.0709 | 0.0576 | 0.0583 | 0.0693     | 0.0780    |
| $[3, 3]; [3, 3, 3, 2]$        | 0.0321 | 0.0238 | 0.0347 | 0.0245 | 0.0356 | 0.0301     | 0.0347    |
| $[3, 9]^4$                    | 0.0361 | 0.0269 | 0.0271 | 0.0273 | 0.0199 | 0.0270     | 0.0219    |
| $[3, 27]; [3, 3, 27]^2$       | 0.0201 | 0.0285 | 0.0302 | 0.0288 | 0.0228 | 0.0263     | 0.0390    |
| $[3, 9]; [3, 3, 3, 27]^2$     | 0.0341 | 0.0254 | 0.0362 | 0.0115 | 0.0256 | 0.0260     | 0.0325    |
| $[3, 9]; [3, 3, 3]^4$         | 0.0402 | 0.0301 | 0.0226 | 0.0101 | 0.0128 | 0.0219     | 0.0195    |
| $[3, 9, 27]; [3, 27]^4$       | 0.0321 | 0.0174 | 0.0166 | 0.0144 | 0.0171 | 0.0188     | 0.0195    |
| $[3, 3, 3, 3]^3$              | 0.0100 | 0.0190 | 0.0196 | 0.0129 | 0.0213 | 0.0169     | 0.0195    |
| $[3, 9, 27]; [3, 27]^3$       | 0.0120 | 0.0206 | 0.0121 | 0.0173 | 0.0185 | 0.0163     | 0.0173    |
| Other IPADs (49 types)         | 0.0402 | 0.0967 | 0.0845 | 0.1036 | 0.1010 | 0.0878     |           |
| Incomplete IPADs              | 0.0301 | 0.0761 | 0.1101 | 0.1755 | 0.2162 | 0.1285     |           |

A complete file containing the fields (listed by discriminant) along with the corresponding IPAD data (complete or partial) and defining polynomials for the extensions can be obtained by following links on the authors’ web pages. We are in the process of attempting to capture some of the fields with incomplete IPAD data by increasing the time limit.

Acknowledgements. We acknowledge useful correspondence and conversations with Bettina Eick, Jordan Ellenberg, Cam McLeman, Eamonn O’Brien, and Melanie Matchett Wood. We are grateful to Jonathan Blackhurst for providing the Appendix. We would also like to thank Joann Boston for drawing the figure in Section 2.

Appendix. On the nucleus of certain $p$-groups

Jonathan Blackhurst

In this appendix we prove the proposition that if the Schur multiplier of a finite non-cyclic $p$-group $G$ is trivial, then the nucleus of $G$ is trivial. Our proof of the proposition will use the facts that a $p$-group has trivial nucleus if and only if it has no immediate descendants and that a finite group has trivial Schur multiplier if and only if it has no non-trivial stem extensions, so we will begin by recalling a few definitions. For the definition of the lower $p$-central series and $p$-class of a group, we refer to section 2 of the article.

Definition. Let $G$ be a finite $p$-group with minimal number of generators $d = d(G)$ and presentation $F/R$ where $F$ is the free pro-$p$ group on $d$ generators. The $p$-covering group $G^c$ of $G$ is
Heuristics for $p$-class Towers of Imaginary Quadratic Fields

$F/R^*$ where $R^*$ is the topological closure of $R^*[F,R]$, and the nucleus of $G$ is $P_e(G^*)$ where $e$ is the $p$-class of $G$. The $p$-multiplier of $G$ is defined to be the subgroup $R/R^*$ of $G^*$. The Schur multiplier $M(G)$ of $G$ is defined to be $(R \cap [F,F])/[F,R]$. A group $C$ is a stem extension of $G$ if there is an exact sequence

$$1 \to K \to C \to G \to 1$$

where $K$ is contained in the intersection of the center and derived subgroups of $C$.

We will need to recall some basic properties of Schur multipliers and $p$-covering groups. First, for a finite group $G$, the largest stem extension of $G$ has size $|G||M(G)|$. Hence, the Schur multiplier of a finite group $G$ is trivial if and only if $G$ admits no non-trivial stem extensions. Second, every elementary abelian central extension of $G$ is a quotient of $G^*$. By this we mean that if $H$ is a $d$-generated $p$-group with elementary abelian subgroup $Z$ contained in the center of $H$ such that $H/Z$ is isomorphic to $G$, then $H$ is a quotient of $G^*$. Every immediate descendant of $G$ is an elementary abelian central extension of $G$, hence is a quotient of $G^*$. A subgroup $M$ of the $p$-multiplier of $G$ is said to supplement the nucleus if $M$ and the nucleus together generate the $p$-multiplier, that is $MP_e(G^*) = R/R^*$. The immediate descendants of $G$ can be put in one-to-one correspondence with equivalence classes of proper subgroups $M$ of the $p$-multiplier of $G$ that supplement the nucleus. The equivalence relation comes from the action of the outer automorphism group of $G^*$, so $M$ and $N$ are equivalent if there is an outer automorphism $\sigma$ of $G^*$ such that $\sigma(M) = N$. The reader is referred to O'Brien [19] for more details.

With these preliminaries in place, we can show that the non-cyclic hypothesis in our proposition is necessary by considering the finite cyclic $p$-group $G = \mathbb{Z}/p^e\mathbb{Z}$. The Schur multiplier is trivial since in this case $F = \mathbb{Z}$ so $[F,F]$ is trivial. On the other hand, the nucleus is non-trivial since in this case $F = \mathbb{Z}_p$ and $R = p\mathbb{Z}_p$ so $R^* = p^{e+1}\mathbb{Z}_p$ and $G^* = F/R^* = \mathbb{Z}/p^{e+1}\mathbb{Z}$ which implies that $P_e(G^*) = p^eG^*$ is non-trivial.

**Proposition:** Let $G$ be a finite non-cyclic $p$-group. If the Schur multiplier of $G$ is trivial, then the nucleus of $G$ is trivial.

**Proof.** We will prove the following equivalent assertion: if the nucleus of $G$ is non-trivial, then $G$ has a non-trivial stem extension. We divide the problem into two cases depending on whether the abelianization of $G$ has stabilized; that is, whether the abelianization of an immediate descendant of $G$ can have larger order than the abelianization $G^{ab}$ of $G$. We will see that this is equivalent to whether or not $G^{ab} \simeq (G/P_{c-1}(G))^{ab}$ where $G$ has $p$-class $c$.

**CASE 1:** Suppose that $G^{ab} \simeq (G/P_{c-1}(G))^{ab}$ and that the nucleus of $G$ is non-trivial. Since the nucleus is non-trivial, $G$ has an immediate descendant $C$ and we have the following diagram

$$1 \to K \to C \to G \to 1$$

where $K = P_1(C)$. Note that since $C/P_k(C) \simeq G/P_k(G)$ for $k \leq c$, we have that $(C/P_{c-1}(C))^{ab} \simeq (C/K)^{ab}$. If $P_{c-1}(C)$ were not contained within the derived subgroup $C'$ of $C$, then its image $\overline{P_{c-1}(C)}$ in $C/C'$ would be non-trivial. Since $K = P_{c-1}(C)^p[C,P_{c-1}(C)]$, the image $\overline{K}$ of $K$ would be $\overline{P_{c-1}(C)}^p$ and thus would be strictly smaller than $\overline{P_{c-1}(C)}$. Now $(C/H)^{ab} \simeq (C/C'/H)$ for any $H \triangleleft C$, so, replacing $H$ with $K$ and $P_{c-1}(C)$, we see that $(C/P_{c-1}(C))^{ab}$ would be smaller than $(C/K)^{ab}$, contradicting that they are isomorphic. Thus $P_{c-1}(C) < C'$, hence $K < C'$, so $C$ is a stem extension of $G$. Since $G$ has a non-trivial stem extension, its Schur multiplier is non-trivial.
CASE 2: Suppose that $G^{ab} \not\cong (G/P_{c-1}(G))^{ab}$. Let

$$1 \to R \to F \to G \to 1$$

be a presentation of $G$ where $F$ is free pro-$p$ group on $d$ generators and $d$ is the minimal number of generators of $G$. Induction and the argument in the preceding case shows that $(G/P_k(G))^{ab}$ is strictly smaller than $(G/P_{k+1}(G))^{ab}$ for any $k < c$. Furthermore, since the image $P_{k+1}(G)$ of $P_k(G)$ in $G/G'$ is a normal subgroup of $G'$, there must be a generator $b$ of $F$ such that the image of $b^{p^{c-1}}$ in $G$ lies outside $G'$. Now consider $R^* = R^p[F,R]$ and let $G^* = F/R^*$ be the $p$-covering group of $G$. We have the following diagrams:

$$1 \to R^* \to F \to G^* \to 1$$

and

$$1 \to R/R^* \to G^* \to G \to 1$$

We now show that the image of $b^{p^c}$ in $P_c(G^*)$ is non-trivial so $G$ has non-trivial nucleus. Let $G$ have abelianization isomorphic to $\mathbb{Z}/p^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_d}\mathbb{Z}$. Consider the topological closure $S$ of $R \cup [F,F]$. Then $F/S$ is isomorphic to $C^{ab}$. The group $\mathbb{Z}/p^{n_1+1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_d+1}\mathbb{Z}$ is an elementary abelian central extension of $F/S$. This implies that $b^{p^c}$ lies outside $S^* = S^p[F,S]$. Hence $b^{p^c}$ lies outside $R^*$ so it has non-trivial image in $G^*$. Since its image lies inside $P_c(G^*)$, this group is non-trivial.

We have shown that $G$ has non-trivial nucleus. Now let $a$ be a generator of $F$ independent of $b$—i.e., one that doesn’t map to the same element as $b$ in the elementary abelianization of $F$—and let $\overline{M}$ be a proper subgroup of $R/R^*$ that contains the image of $b^{p^c}[a,b^{p^{c-1}}]$ and that supplements the subgroup of $R/R^*$ generated by the image of $b^{p^c}$ (so $\overline{M}$ and the image of $b^{p^c}$ generate $R/R^*$). Now consider $C = G^*/\overline{M}$. Letting $K = (R/R^*)/\overline{M}$, we have the following diagram

$$1 \to K \to C \to G \to 1$$

Since $G^*$ is a central extension of $G$ and $C$ is a quotient of $G^*$, $C$ is also a central extension of $G$. Furthermore, $|K| = p$. Now let $M$ be the subgroup of $F$ corresponding to $\overline{M}$ under the lattice isomorphism theorem. Then we have the following diagram:

$$1 \to M \to F \to C \to 1$$

Since $M$ does not contain $b^{p^c}$, its image in $C$ is non-trivial. Since $G$ has $p$-class $c$, the image of $b^{p^c}$ is trivial in $G$. Also since $|K| = p$, the image of the powers of $b^{p^c}$ constitute $K$. Since $M$ does contain $b^{p^c}[a,b^{p^{c-1}}]$, the image of $b^{p^c}$ in $C$ equals the image of $[b^{p^{c-1}},a]$, hence $K$ lies in the derived subgroup of $C$, so $C$ is a non-trivial stem extension of $G$. Consequently, the Schur multiplier of $G$ is non-trivial. 

\[\square\]

REFERENCES

1. L. Bartholdi and M.R. Bush, Maximal unramified 3-extensions of imaginary quadratic fields and $SL_2(\mathbb{Z}_3)$, J. Number Theory 124 (2007), no. 1, 159–166.

2. M. Bhargava, The density of discriminants of quartic rings and fields Ann. of Math. (2) 162 (2005), no. 2, 10311063.

3. W. Bosma, J. J. Cannon, C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput., 24 (1997), 235–265.
Heuristics for $p$-class Towers of Imaginary Quadratic Fields

4 N. Boston, *Explicit deformation of Galois representations*, Inventiones. Mathematicae 103 (1991), 181–196.

5 N. Boston, *Random pro-$p$ groups and random Galois groups*, Annales des Sciences Mathématiques du Québec. 32 (2008), no. 2, 125–138.

6 N. Boston and J. Ellenberg, *Random pro-$p$ groups, braid groups, and random tame Galois groups*, Groups Geom. Dyn. 5 (2011), no. 2, 265-280.

7 N. Boston and C.R. Leedham-Green, *Explicit computation of Galois $p$-groups unramified at $p$*, Journal of Algebra 256 (2002), no. 2, 402–413.

8 N. Boston and H. Nover, *Computing pro-$p$ Galois groups*, Lecture Notes in Computer Science 4076, ANTS VII, 1-10.

9 H. Cohen and H.W. Lenstra, Jr., *Heuristics on class groups*, in: Number Theory, 26–36, LNM 1052, Springer, Berlin, 1984.

10 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.

11 H. Cohen and J. Martinet, *Étude heuristique des groupes des classes des corps de nombres*, J. Reine Angew. Math. 404 (1990), 39–76.

12 H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields (ii)*, Proc. Roy. Soc. Lond. A 322 (1971), 405–420.

13 E. Friedman and L. C. Washington, *On the distribution of divisor class groups of curves over a finite field*, Théorie des nombres (Quebec, PQ, 1987), 227–239, de Gruyter, Berlin, 1989.

14 D. Gildenhuys, W. Herfort, and L. Ribes, *Profinite Frobenius groups*, Arch. Math. (Basel) 33 (1979/80), no. 6, 518–528.

15 P. Hall, *A contribution to the theory of groups of prime-power order*, Proc. London Math. Soc. 36 (1934), 29–95.

16 P. Hall, *A partition formula connected with Abelian groups*, Comment. Math. Helv. 11 (1938-39), 126-129.

17 H. Koch and B.B. Venkov, *Über den $p$-Klassenkörperturm eines imaginär-quadratischen Zahlkörpers*, Soc. Math. France, Astérique 24-25 (1975), 57–67.

18 C. McLeman, *Class field towers over quadratic imaginary number fields*, Annales des Sciences Mathématiques du Québec 32 (2008), no 2, 199–209.

19 E.A. O'Brien, *The $p$-group generation algorithm*, J. Symbolic Comput. 9 (1990), 677–698.

20 A. Scholz and O. Taussky, *Die Hauptideale der kubischen Klassenkörper imaginär-quadratischer Zahlkörper*, J. Reine Angew. Math. 171 (1934), 19–41.

21 I. Shafarevich, *Extensions with prescribed ramification points*, Inst. Hautes Études Sci. Publ. Math. 18 (1964), 7195 [In Russian]; English translation “Amer. Math. Soc. Transl.,” Vol. 59, pp. 128149, Amer. Math. Soc., Providence, RI, 1966.

22 C. Wittmann, *$p$-class groups of certain extensions of degree $p$*, Math. Comp. 74 (2005), no. 250, 937-947.

Jonathan Blackhurst  blackhur@math.wisc.edu
Department of Mathematics, University of Wisconsin - Madison, 480 Lincoln Drive, Madison, WI 53706, USA

Nigel Boston  boston@math.wisc.edu
Department of Mathematics, University of Wisconsin - Madison, 480 Lincoln Drive, Madison, WI 53706, USA
