MISSING CLASS GROUPS AND CLASS NUMBER STATISTICS FOR IMAGINARY QUADRATIC FIELDS

S. HOLMIN, N. JONES, P. KURLBERG, C. MCLEMAN AND K. PETERSEN

Abstract. The number $\mathcal{F}(h)$ of imaginary quadratic fields with class number h is of classical interest: Gauss' class number problem asks for a determination of those fields counted by $\mathcal{F}(h)$. The unconditional computation of $\mathcal{F}(h)$ for $h \leq 100$ was completed by Watkins, using ideas of Goldfeld and Gross-Zagier; Soundararajan has more recently made conjectures about the order of magnitude of $\mathcal{F}(h)$ as $h \to \infty$ and determined its average order. In the present paper, we refine Soundararajan's conjecture to a conjectural asymptotic formula for odd h by amalgamating the Cohen-Lenstra heuristic with an archimedean factor, and obtain an adelic, or global, refinement of the Cohen-Lenstra heuristic.

We also consider the problem of determining the number $\mathcal{F}(G)$ of imaginary quadratic fields with class group isomorphic to a given finite abelian group G. Using Watkins' tables, one can show that some abelian groups do *not* occur as the class group of any imaginary quadratic field (for instance $(\mathbb{Z}/3\mathbb{Z})^3$ does not). This observation is explained in part by the Cohen-Lenstra heuristics, which have often been used to study the distribution of the *p-part* of an imaginary quadratic class group. We combine heuristics of Cohen-Lenstra together with our prediction for the asymptotic behavior of $\mathcal{F}(h)$ to make precise predictions about the asymptotic nature of the *entire* imaginary quadratic class group, in particular addressing the above-mentioned phenomenon of "missing" class groups, for the case of p-groups as p tends to infinity. Furthermore, conditionally on the Generalized Riemann Hypothesis, we extend Watkins' data, tabulating $\mathcal{F}(h)$ for odd $h \leq 10^6$ and $\mathcal{F}(G)$ for G a p-group of odd order with $|G| \leq 10^6$. (In order to do this, we need to examine the class numbers of all negative prime fundamental discriminants $-q$, for $q \leq 1.1881 \cdot 10^{15}$.) The numerical evidence matches quite well with our conjectures, though there appears to be a small "bias" for class number divisible by powers of 3.

1. Introduction

Given a fundamental discriminant $d < 0$, let $H(d)$ denote the ideal class group of the imaginary quadratic field $\mathbb{Q}(\sqrt{d})$, and let $h(d) := |H(d)|$ denote the class number. A basic question is:

Question 1.1. Which finite abelian groups G occur as $H(d)$ for some negative fundamental discriminant d?

Equivalently, which finite abelian groups G do *not* occur as $H(d)$? The case where $G \simeq (\mathbb{Z}/2\mathbb{Z})^r$ has classical connections via genus theory to Euler's "idoneal numbers," and it follows from work of Chowla [8] that for every $r \gg 1$, the group $(\mathbb{Z}/2\mathbb{Z})^r$ does not occur as the class group of any imaginary quadratic field. Later work of various authors ([6], [49], [18]) has shown that $(\mathbb{Z}/n\mathbb{Z})^r$ does not occur as an imaginary quadratic class group for $r \gg 1$ and $2 \leq n \leq 6$ (in fact, Heath-Brown showed that groups with exponent 2^a or $3 \cdot 2^a$ occur only finitely many times.) Moreover, $(\mathbb{Z}/n\mathbb{Z})^r$ does not occur for $n > 6$ and $r \gg_n 1$ *assuming* the Generalized Riemann Hypothesis (cf. [6, 49]); in fact they show that the exponent of $H(d)$ tends to infinity as $d \to -\infty$.

Due to the possible existence of Siegel zeroes, the unconditional results mentioned above are ineffective. To find explicit examples of missing class groups, one can undertake a brute-force search using tables of M. Watkins [48], who used the ideas of Goldfeld and Gross-Zagier to give an unconditional resolution of Gauss' class number problem for class numbers $h \leq 100$. Such a search reveals that none of the groups $(\mathbb{Z}/3\mathbb{Z})^3, \mathbb{Z}/9\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2, (\mathbb{Z}/3\mathbb{Z})^4$ occur as the class group of an imaginary quadratic field.

It is also natural to ask how common the groups that do occur are:

Question 1.2. Given a finite abelian group G, for how many fundamental discriminants $d < 0$ is $H(d) \simeq G$?

2010 *Mathematics Subject Classification.* 11R29, 11Y40.

Key words and phrases. Class numbers, class groups, Cohen-Lenstra heuristics.

In order to address this question, we are led to investigate a closely related issue:

Question 1.3. Given an integer $h > 0$, for how many fundamental discriminants $d < 0$ is $|H(d)| = h$?

Questions 1.1, 1.2, and 1.3 appear to be beyond the realm of what one can provably answer in full with current technology. In this paper, we combine the heuristics of Cohen-Lenstra with results on the distribution of special values of Dirichlet L-functions to give a conjectural asymptotic answer to Question 1.3, for h odd. (For this we only use the Cohen-Lenstra heuristic to predict divisibility properties of class numbers.) Further, using this conjectured asymptotic answer, we use the Cohen-Lenstra heuristic to predict the p-group decomposition of $H(d)$ and obtain a conjectured asymptotic answer to Question 1.2 in the case where G is a p-group for an odd prime p. (We believe that similar results hold for composite class number, though here one must be careful in how limits are taken; for instance with some groups of order $p_1^{n_1}p_2^{n_2}$, p_1 fixed and p_2 tending to infinity is very different from p_1 and p_2 both tending to infinity.)

In particular, regarding Question 1.1, we establish a precise condition on the *shape* of an abelian p-group which governs whether or not it should occur as an imaginary quadratic class group for infinitely many primes p. For instance, our conjecture predicts that the group $(\mathbb{Z}/p\mathbb{Z})^3$ should appear as a class group for only finitely many primes p (in fact, quite likely for no primes p at all; cf. Conjecture 1.10 in Section 1.3), whereas the two groups $\mathbb{Z}/p^3\mathbb{Z}$ and $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ should occur as a class group for infinitely many primes p.

Given a positive integer h we set

$$\mathcal{F}(h) := |\{\text{fundamental discriminants } d < 0 \ : \ h(d) = h\}|. \tag{1.1}$$

Thus for instance $\mathcal{F}(1) = 9$, which is the statement of the Baker-Stark-Heegner theorem on Gauss' class number 1 problem for imaginary quadratic fields. Given a fixed finite abelian group G, we consider the refined counting function

$$\mathcal{F}(G) := |\{\text{fundamental discriminants } d < 0 \ : \ H(d) \simeq G\}|,$$

so that $\mathcal{F}(h) = \sum_{|G|=h} \mathcal{F}(G)$, where the sum runs over isomorphism classes of finite abelian groups of order h. The Cohen-Lenstra heuristics suggest that, for any finite abelian group G of odd order h, the expected number of imaginary quadratic fields with class group G is given by

$$\mathcal{F}(G) \approx P(G) \cdot \mathcal{F}(h), \tag{1.2}$$

where

$$P(G) := \left(\frac{1}{|\operatorname{Aut}(G)|}\right) \Bigg/ \left(\sum_{\substack{\text{abel. groups } G' \\ \text{s.t. } |G'|=|G|}} \frac{1}{|\operatorname{Aut}(G')|}\right). \tag{1.3}$$

The first factor $P(G)$ may be evaluated explicitly, whereas the second factor $\mathcal{F}(h)$ is more delicate. K. Soundararajan has conjectured (see [44, p. 2]) that

$$\mathcal{F}(h) \asymp \frac{h}{\log h} \qquad (h \text{ odd}). \tag{1.4}$$

We refine Soundararajan's heuristic, sharpening (1.4) to a conjectural asymptotic formula, which involves certain constants associated to a random Euler product. Let $\mathbb{Y} = \{\mathbb{Y}(p) : p \text{ prime}\}$ denote a collection of independent identically distributed random variables satisfying

$$\mathbb{Y}(p) := \begin{cases} 1 & \text{with probability } 1/2 \\ -1 & \text{with probability } 1/2 \end{cases}$$

and let

$$L(1, \mathbb{Y}) := \prod_p \left(1 - \frac{\mathbb{Y}(p)}{p}\right)^{-1}$$

denote the corresponding random Euler product, which converges with probability one. Define the constant

$$\mathfrak{C} := 15 \prod_{\substack{\ell=3 \\ \ell \text{ prime}}}^{\infty} \prod_{i=2}^{\infty} \left(1 - \frac{1}{\ell^i}\right) \approx 11.317, \tag{1.5}$$

as well as the factor (defined for odd h)

$$\mathfrak{c}(h) := \prod_{p^n \| h} \prod_{i=1}^{n} \left(1 - \frac{1}{p^i}\right)^{-1}.$$

Conjecture 1.4. *We have*

$$\mathcal{F}(h) \sim \frac{\mathfrak{C}}{15} \cdot \mathfrak{c}(h) \cdot h \cdot \mathbb{E}\left(\frac{1}{L(1,\mathbb{Y})^2 \log(\pi h / L(1,\mathbb{Y}))}\right) \sim \mathfrak{C} \cdot \mathfrak{c}(h) \cdot \frac{h}{\log(\pi h)} \tag{1.6}$$

as $h \longrightarrow \infty$ through odd values. (Here $\mathbb{E}$ denotes expected value.)

Remark 1.5. The second asymptotic in (1.6) may be seen as the first term in an asymptotic expansion, and in fact our analysis (cf. Section 6) yields the more accurate approximation

$$\begin{aligned} \mathcal{F}(h) &\sim \frac{\mathfrak{C}}{15} \cdot \mathfrak{c}(h) \cdot h \cdot \mathbb{E}\left(\frac{1}{L(1,\mathbb{Y})^2 \log(\pi h / L(1,\mathbb{Y}))}\right) \\ &= \mathfrak{C} \cdot \mathfrak{c}(h) \cdot \frac{h}{\log(\pi h)} \cdot \left(1 + \frac{c_1}{\log(\pi h)} + \frac{c_2}{\log^2(\pi h)} + \frac{c_3}{\log^3(\pi h)} + o\left(\frac{1}{\log^3(\pi h)}\right)\right), \end{aligned} \tag{1.7}$$

where

$$\begin{aligned} c_1 &:= \frac{\pi^2}{15}\mathbb{E}\left(\frac{\log L(1,\mathbb{Y})}{L(1,\mathbb{Y})^2}\right) \approx -0.578, \\ c_2 &:= \frac{\pi^2}{15}\mathbb{E}\left(\frac{\log^2 L(1,\mathbb{Y})}{L(1,\mathbb{Y})^2}\right) \approx 0.604, \\ c_3 &:= \frac{1}{c_0}\mathbb{E}\left(\frac{\log^3 L(1,\mathbb{Y})}{L(1,\mathbb{Y})^2}\right) \approx -0.526. \end{aligned} \tag{1.8}$$

Without this higher order expansion we have a relative error of size $O(1/\sqrt{\log h})$; since we only have data for odd $h \leq 10^6$, the higher order expansion is essential to get a convincing fit to the observed data.

Conjecture 1.4 is developed from the Cohen-Lenstra heuristics together with large-scale distributional considerations of the special value $L(1, \chi_d)$. The former can be viewed as a product over non-archimedean primes; the latter as an archimedean factor — in a sense our prediction is a "global" (or adelic) generalization of the Cohen-Lenstra heuristic, somewhat similar to the Siegel mass formula.

More precisely, motivated by the Cohen-Lenstra heuristic we introduce a correction factor that considers divisibility of h by a random odd positive integer (for instance a random class number is divisible by 3 with conjectural probability

$$1 - \prod_{i=1}^{\infty}\left(1 - \frac{1}{3^i}\right) \approx 43\%,$$

and this suggests a correction factor of $\left(1 - \prod_{i=1}^{\infty}\left(1 - \frac{1}{3^i}\right)\right)/(1/3)$ whenever 3 divides h). We remark that the Cohen-Lenstra heuristics have often been applied to give a probabilistic model governing the *p-part* of a class group, for a *fixed* prime p (see for instance [11, Section 9]). By contrast, the precise asymptotic predicted by Conjecture 1.4 involves applying these considerations for *all* primes p (including the archimedean prime).

The relevant information about the distribution of $L(1, \chi_d)$ is implicit in the following theorem, which gives the analogue of [44, Theorem 1] averaged over odd values of h.

Theorem 1.6. *Assume the Generalized Riemann Hypothesis for Dirichlet L-functions. Then for any $\varepsilon > 0$, we have*

$$\sum_{\substack{h \leq H \\ h \text{ odd}}} \mathcal{F}(h) = \frac{15}{4} \cdot \frac{H^2}{\log H} + O\left(H^2 (\log H)^{-3/2+\varepsilon}\right),$$

as $H \longrightarrow \infty$.

We remark that Theorem 1.6 has been improved by Lamzouri. Without hypothesis he shows that the error term is $O(H^2(\log\log H)^3/(\log H)^{3/2})$ (cf. [27]); on GRH he obtains the error term $O(H^2(\log\log H)^3/(\log H)^2)$ (cf. [26]).

1.1. **Numerical evidence for Conjecture 1.4.** With the aid of a supercomputer and assuming GRH, we have computed $\mathcal{F}(h)$ and $\mathcal{F}(G)$ for all odd $h < 10^6$ and all p-groups G of odd size at most 10^6 (for more details, see Section 9.) In particular, we *conditionally* extend the class number computation [24], where Jacobson, Ramachandran, and Williams unconditionally determine $h(-d)$ for $d < 10^{11}$, and $-d$ a fundamental discriminant; recently Mosunov and Jacobson further extended [32] this range to $d < 2^{40}$. The numerics give us quite convincing evidence in support of Conjecture 1.4. Below we give some samples[1] of computed values $\mathcal{F}(h)$ (conditional on the GRH) compared to the values predicted by Conjecture 1.4, rounded to the nearest integer. We also list the relative error $(\mathcal{F}(h) - \operatorname{pred}(h)) / \operatorname{pred}(h)$ given as a percentage, where

$$\operatorname{pred}(h) := \mathfrak{C} \cdot \mathfrak{c}(h) \cdot \frac{h}{\log(\pi h)} \cdot \left(1 + \frac{c_1}{\log(\pi h)} + \frac{c_2}{\log^2(\pi h)} + \frac{c_3}{\log^3(\pi h)}\right). \tag{1.9}$$

h	10001	10003	10005	10007	10009	10011	10013	10015
$\mathcal{F}(h)$	10641	12154	20661	10536	10329	15966	12221	12975
pred(h)	10598	12116	21074	10383	10385	16144	12038	12993
Relative error	+0.41%	+0.31%	−1.96%	+1.48%	−0.54%	−1.10%	+1.52%	−0.14%

h	100001	100003	100005	100007	100009	100011	100013	100015
$\mathcal{F}(h)$	94623	85792	164289	86770	111948	142512	87138	108993
pred(h)	94213	85641	164806	86620	111210	142989	86577	108820
Relative error	+0.43%	+0.18%	−0.31%	+0.17%	+0.66%	−0.33%	+0.65%	+0.16%

h	999985	999987	999989	999991	999993	999995	999997	999999
$\mathcal{F}(h)$	1064529	1095135	771805	791007	1093645	914482	733397	1815672
pred(h)	1063376	1098842	769673	788871	1093732	911447	730673	1825811
Relative error	+0.11%	−0.34%	+0.28%	+0.27%	−0.01%	+0.33%	+0.37%	−0.56%

For large h the prediction seems fairly good as the relative error very often is smaller than 1%. To gain further insight, we study the fluctuations in the difference between the observed data and the predictions, normalized by dividing by the square root of the prediction (it is perhaps not a priori obvious, but with this normalization the resulting standard deviation is close to one in many circumstances). More precisely, we make a histogram of the values of

$$r(h) := \frac{\mathcal{F}(h) - \operatorname{pred}(h)}{\sqrt{\operatorname{pred}(h)}}$$

for various subsets of the (odd) integers. For notational convenience, we shall let μ and σ denote the mean and standard deviation, respectively, of the observed data in each plot.

[1] The complete list of computed values of $\mathcal{F}(h)$ is given in [21].

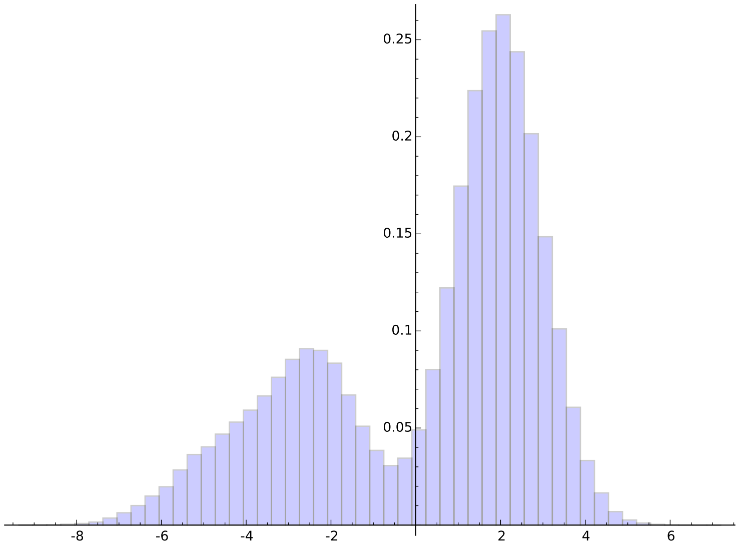


Figure 1. Histogram for $r(h)$, as h ranges over odd integers in $[500000, 1000000]$. $(\mu, \sigma) = (0.291561, 2.685280)$.

Interestingly, the probability distribution appears to be bimodal. A closer inspection of the table above indicates a small positive bias for h that are divisible by three. Separating out (odd) h according to divisibility by three, or not, results in the following two histograms:

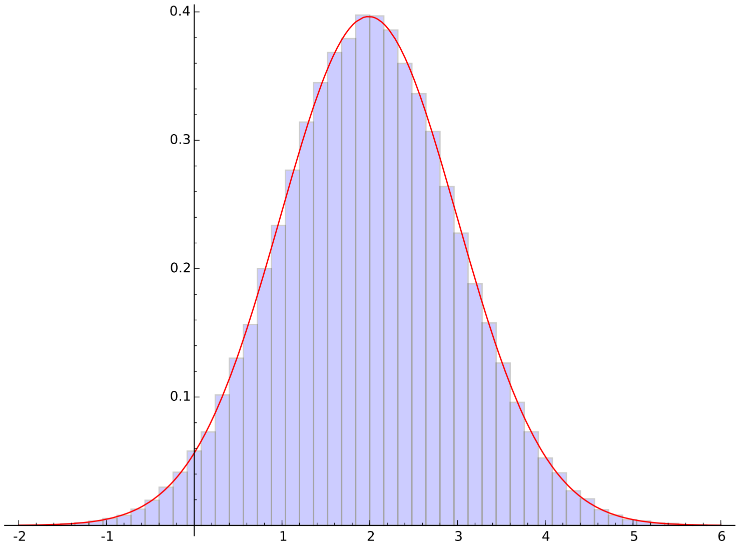


Figure 2. Histogram for $r(h)$, as $h \not\equiv 0 \bmod 3$ ranges over odd integers in $[500000, 1000000]$. $(\mu, \sigma) = (1.987995, 1.006428)$.

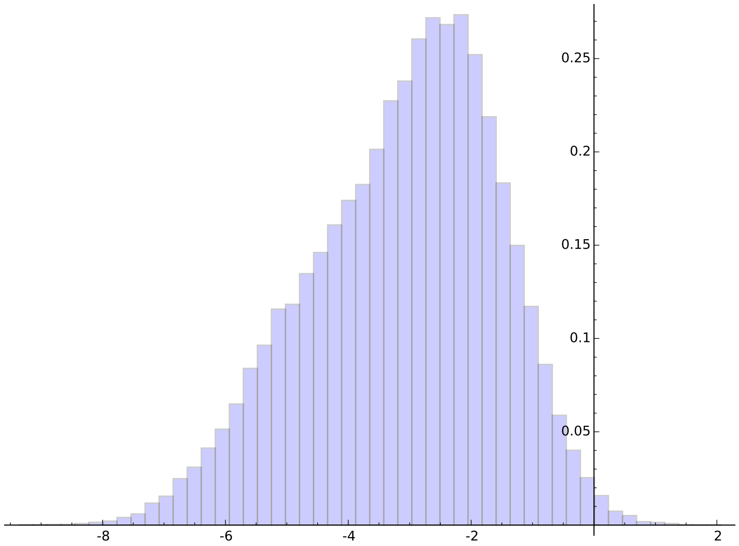


FIGURE 3. Histogram for $r(h)$, as $h \equiv 0 \bmod 3$ ranges over odd integers in $[500000, 1000000]$. $(\mu, \sigma) = (-3.101265, 1.529449)$.

The curve (red in color printouts and online) in the first plot is a Gaussian probability density function with mean and standard deviation fitted to the data — the first plot appears to be Gaussian, whereas the second clearly is not. We note that (after our normalization), the effect of three divisibility is quite pronounced — the shift in the mean value is of order of magnitude a standard deviation. We believe that this "three divisibily bias" is related to a certain lower order correction in the Davenport-Heilbronn asymptotic; for more details on this together with further numerics, see Section 2.

1.2. **Groups occuring as class groups.** We now return to our discussion of the quantity $\mathcal{F}(G)$. To make precise what we mean by the *shape* of an abelian p-group, recall the bijection

$$\{\text{partitions of } n\} \leftrightarrow \{\text{abelian groups of order } p^n\}$$

$$\lambda = (n_1, n_2, \ldots, n_r) \mapsto G_\lambda(p) := \bigoplus_{i=1}^{r} \mathbb{Z}/p^{n_i}\mathbb{Z}.$$

Using (1.2) in conjunction with Conjecture 1.4, and evaluating each factor asymptotically, we are led to the following conjecture. Given a partition

$$\lambda = (n_1, n_2, \ldots, n_r), \quad n_1 \geq n_2 \geq \cdots \geq n_r \geq 1, \quad n_1 + n_2 + \cdots + n_r = n$$

of n, define the *cyclicity index* of λ by

$$\mathrm{c}(\lambda) := \sum_{i=1}^{r} (3 - 2i) n_i = n_1 - \sum_{i=2}^{r} (2i - 3) n_i. \tag{1.10}$$

Note that $\mathrm{c}(\lambda) \in [1 - (n-1)^2, n]$ and $G_\lambda(p)$ is cyclic if and only if $\mathrm{c}(\lambda) = n$; thus $\mathrm{c}(\lambda)$ provides a measure of how much $G_\lambda(p)$ deviates from being cyclic.

Conjecture 1.7. *Fix $n \in \mathbb{N}$ and a partition λ of n. Then $\mathcal{F}(G_\lambda(p)) > 0$ for infinitely many primes p if and only if $\mathrm{c}(\lambda) \geq 0$. More precisely, if $\mathrm{c}(\lambda) > 0$ then as $p \to \infty$ we have*

$$\mathcal{F}(G_\lambda(p)) \sim \frac{\mathfrak{C}}{n} \cdot \frac{p^{\mathrm{c}(\lambda)}}{\log p},$$

where $\mathfrak{C}$ is as in (1.5). If $\mathrm{c}(\lambda) = 0$ then as $x \to \infty$ we have

$$\sum_{\substack{p \leq x \\ p \text{ prime}}} \mathcal{F}(G_\lambda(p)) \sim \frac{\mathfrak{C}}{n} \cdot \frac{x}{(\log x)^2}.$$

If $\mathrm{c}(\lambda) < 0$ *then*

$$p \gg_\lambda 1 \implies \mathcal{F}(G_\lambda(p)) = 0.$$

Definition 1.8. We say that a partition λ of n is *attainable* if $\mathrm{c}(\lambda) \geq 0$.

Thus, Conjecture 1.7 implies that $G_\lambda(p)$ occurs as a class group for infinitely many primes p if and only if λ is attainable. Our next theorem shows that rather few types of groups are attainable — the relative proportion of attainable partitions among all partitions tends to zero as n grows.

Theorem 1.9. *For a positive integer* n, *we have*

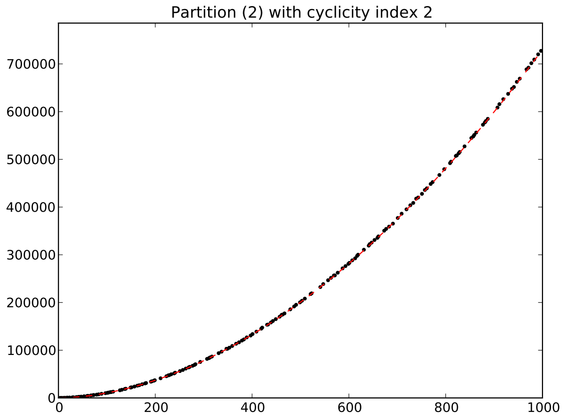
$$\frac{\#\{\textit{attainable partitions of } n\}}{\#\{\textit{partitions of } n\}} \ll n^{3/4} e^{(2-\sqrt{\frac{2}{3}}\pi)\sqrt{n}}.$$

In particular,

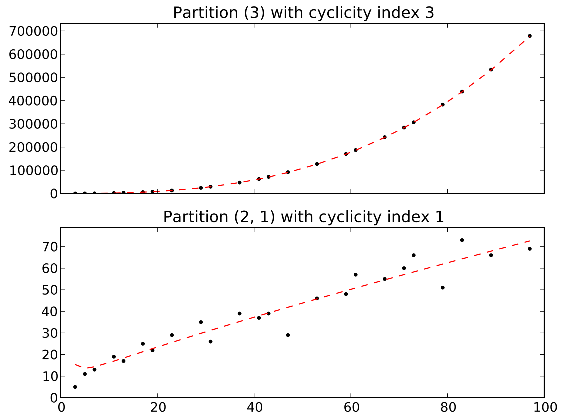
$$\lim_{n\to\infty} \frac{\#\{\textit{attainable partitions of } n\}}{\#\{\textit{partitions of } n\}} = 0.$$

1.3. **Numerical investigations of attainable groups.** For families of p-groups with $\mathrm{c}(\lambda) > 0$, we expect that many (if not all) groups should occur; in fact $\mathcal{F}(G_\lambda(p))$ should grow with p. On the other hand, there should be very few (if any at all) in case $\mathrm{c}(\lambda) < 0$ — we call these groups "sporadic". The case of $\mathrm{c}(\lambda) = 0$ is intermediate in the sense that infinitely many groups in the family should occur, and infinitely many should not.

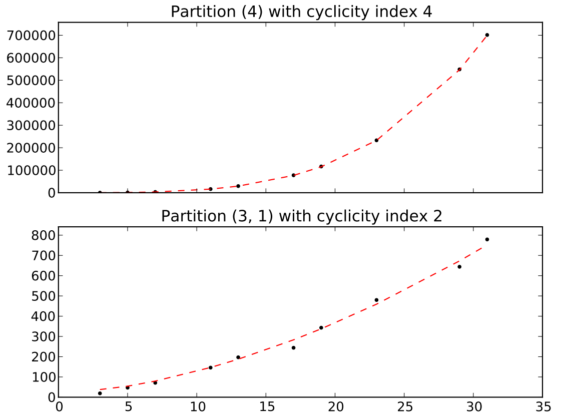
Below we plot, for p ranging over *odd primes*, observed values $\mathcal{F}(G_\lambda(p))$ (black dots) versus predicted values $P(G_\lambda(p)) \cdot \mathrm{pred}(|G_\lambda(p)|)$ (red dashed lines) for various partitions λ with cyclicity index $\mathrm{c}(\lambda) > 0$.



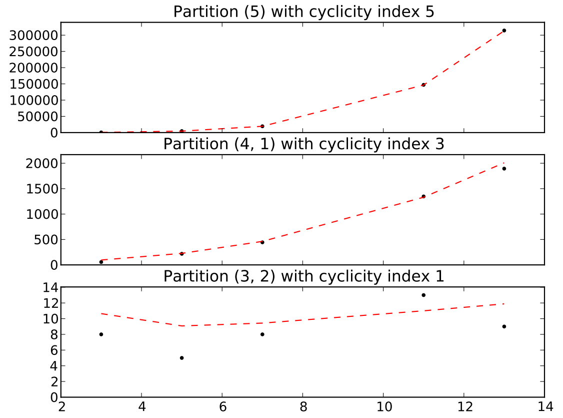
Partitions of 2: $\mathbb{Z}/p^2$



Partitions of 3: $\mathbb{Z}/p^3$ and $\mathbb{Z}/p^2 \times \mathbb{Z}/p$.



Partitions of 4: $\mathbb{Z}/p^4$ and $\mathbb{Z}/p^3 \times \mathbb{Z}/p$.



Partitions of 5: $\mathbb{Z}/p^5, \mathbb{Z}/p^4 \times \mathbb{Z}/p$ and $\mathbb{Z}/p^3 \times \mathbb{Z}/p^2$.

For more details regarding the numerical data, especially when $\mathrm{c}(\lambda) \leq 0$, see Section 3, but we remark that none of the groups $G_\lambda(p)$ of odd size $< 10^6$ with $\mathrm{c}(\lambda) > 0$ are missing. Further, based on a combination of heuristics and numerics, it seems reasonable to conjecture that $(\mathbb{Z}/p\mathbb{Z})^n$ does not occur for any odd prime p and any $n \geq 3$.

Conjecture 1.10. *For p odd, there are no elementary abelian p-groups of rank at least 3 which occur as the class group of an imaginary quadratic field.*

Indeed, by (1.2) and Conjecture 1.4, together with the observed (GRH-conditional) fact that no $(\mathbb{Z}/p\mathbb{Z})^n$ occurs as an imaginary quadratic class group for $p^n \leq 10^6$, we may bound the expected number of counterexamples by

$$\mathfrak{C} \sum_{\substack{p,n \geq 3 \\ p^n > 10^6}} \frac{\mathfrak{c}(p^n)}{np^{n^2-2n}\log p} \leq \mathfrak{C} \cdot \prod_{i=1}^{\infty} \left(1 - \frac{1}{2^i}\right)^{-1} \sum_{\substack{p,n \geq 3 \\ p^n > 10^6}} \frac{1}{np^{n^2-2n}\log p}.$$

Since the right-hand sum can then be bounded by 10^{-4}, Conjecture 1.10 is heuristically justified.

1.4. **Related work.** Certain classes of finite abelian groups are already known *not* to occur as imaginary quadratic class groups. For instance, letting $H(d)[n]$ denote the n-torsion subgroup of $H(d)$, it is known that

$$|H(d)[2]| \ll |H(d)|^{o(1)}$$

(this is essentially genus theory together with Siegel's lower bound on the class number; if $H(d)$ has two rank r, then d has exactly $r+1$ distinct prime factors). In particular, for any fixed $\epsilon > 0$ there are only finitely many imaginary quadratic class groups $H(d)$ satisfying $|H(d)[2]| \gg |H(d)|^{\epsilon}$. Weaker bounds are known for the size of the three torsion part; in [14] Venkatesh and Ellenberg (improving on Helfgott and Venkatesh [19] and Pierce [37]) show that

$$|H(d)[3]| \ll |d|^{1/3+\epsilon}.$$

From this and the (GRH-conditional) lower bound $|d|^{1/2}/\log\log|d| \ll |H(d)|$, one sees that, for any $\epsilon > 0$ there are only finitely many imaginary quadratic class groups $H(d)$ satisfying $|H(d)[3]| \gg |H(d)|^{2/3+\epsilon}$.

The problem of realizing a given abelian group as an imaginary quadratic class group may be viewed in the context of the following broader questions.

Question 1.11. Given a finite abelian group G, does there exist a number field K for which the ideal class group of K is isomorphic to G?

The answer to this problem is believed to be yes (one ought to be able to take K to be a real quadratic extension of $\mathbb{Q}$) but the problem is open in general, in spite of various partial results. G. Cornell [12] proved that every finite abelian group occurs as a subgroup of the ideal class group of some cyclotomic field, and Y. Yamamoto [51] proved that, for any $n \geq 1$, there are infinitely many imaginary quadratic fields whose class group contains $(\mathbb{Z}/n\mathbb{Z})^2$ as a subgroup. We note that Ozaki [34] has shown that any (possibly non-abelian) p-group occurs as the maximal unramified p-extension of some number field F.

Further broadening our perspective, we may also ask:

Question 1.12. Given an abelian group G, does there exist a Dedekind domain D for which the ideal class group of D is isomorphic to G?

In [9], Claborn answered this question in the affirmative; Leedham-Green subsequently showed that the Dedekind domain D can be taken to be a quadratic extension of a principal ideal ring.

Finally, we remark that the Cohen-Lenstra heuristics apply to a broader class of situations where finite abelian groups arise as co-kernels of random sub-lattices of $\mathbb{Z}^n$. For instance, [13] contains average results on the group of $\mathbb{Z}/p\mathbb{Z}$-rational points of an elliptic curve which are consistent with the Cohen-Lenstra heuristics (of course the rank can be at most two in this setting), and (in a similar spirit to our present consideration of missing class groups) [2] considers the question of which finite rank 2 abelian groups occur as the group of $\mathbb{Z}/p\mathbb{Z}$-rational points of some elliptic curve E over $\mathbb{Z}/p\mathbb{Z}$.

We conclude with some remarks regarding the numerical computations. Removing the assumption of GRH and making the computational results unconditional would be interesting, but probably very difficult since effective unconditional lower bounds on class numbers are quite weak (the best know bound, due to

Oesterlé [33], is that $h(-q) \gg \log q$ for $-q$ a negative prime fundamental discriminant.) In particular, it would involve a major advance on Watkin's solution [48] to Gauss' class number problem for $h \leq 100$. (Of course, considering only odd h should be quite helpful.)

Determining $h(-d)$ for $d \in (0, D)$ and $-d$ ranging over fundamental discriminants is somewhat easier to do unconditionally, either by enumerating the primitive reduced quadratic forms in time $O(D^{3/2})$ (cf. [7]), or using GRH-conditional algorithms which, as suggested by A. Booker, can then be verified using the Eichler-Selberg trace formula. The latter algorithm, due to Jacobson, Ramachandran, and Williams [24], leads to a total running time of $O(D^{5/4})$, and allowed them to take $D = 10^{11}$. However, the verification step relies on knowing $h(-d)$ for all d in the relevant range, and seems difficult to adapt to a setting where only $h(-q)$ is known for $0 < q < D$ and $-q$ ranging over negative prime fundamental discriminants. On the other hand, Booker's algorithm [5] gives the correct value of $h(-d)$ in time $O(d^{1/4})$ if GRH is true (in time $O(d^{1/2})$ otherwise), and his algorithm can easily be restricted to prime discriminants. It would also be interesting to investigate the potential speedup from using Sutherland's primorial-steps algorithm (cf. [45, Ch. 4 and 11] — it exploits the smooth part of the class number, and results in better than $O(d^{1/7})$ median time to find $h(-d)$.

1.5. **Outline of the paper.** The organization is as follows: Section 2 discusses the 3-divisibility bias visible in Figures 1, 2 and 3 above, while Section 3 presents further numerical evidence in support of Conjecture 1.7. Section 4 covers the preliminary material on Cohen-Lenstra heuristics and the distribution of $L(1, \chi_d)$. In Section 5, we prove Theorem 1.6. In Section 6, we develop heuristics which lead to Conjectures 1.4 and 1.7. In Section 8, we discuss partition generating functions and give a proof of Theorem 1.9. In Section 9, we sketch the techniques used to obtain the numerical evidence.

2. Fine scale fluctations and the 3-divisibility bias

By further separating $h \equiv 0 \mod 3$ into subsets according to the exact power of three that divides h, we obtain distributions that appear Gaussian; for comparison, we again plot a (red) curve giving the probability density function for a Gaussian random variable with the same mean and standard deviation as the observed data. (Note that there is a significant shift in the mean, whereas the standard deviation is close to one.)

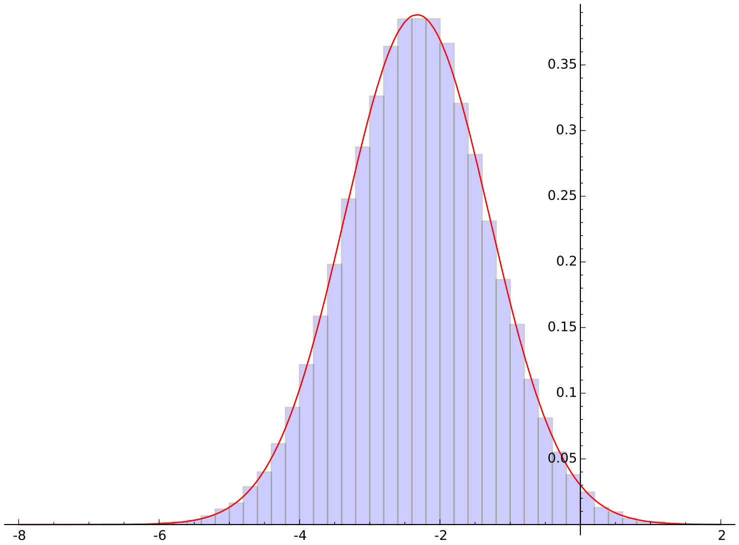


FIGURE 4. Histogram for $r(h)$, for odd h in (500000,1000000), $3||h$. $(\mu, \sigma) = (-2.326289, 1.027387)$.

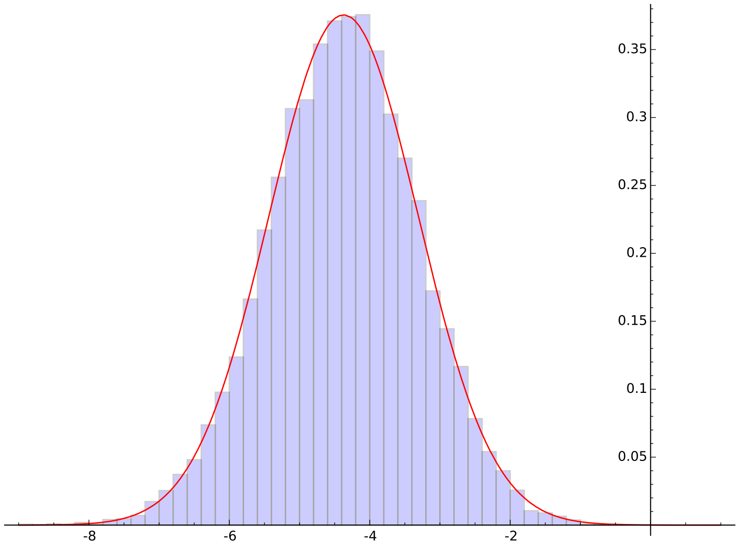


Figure 5. Histogram for $r(h)$, for odd h in (500000,1000000), $3^2||h$. $(\mu, \sigma) = (-4.372185, 1.062480)$.

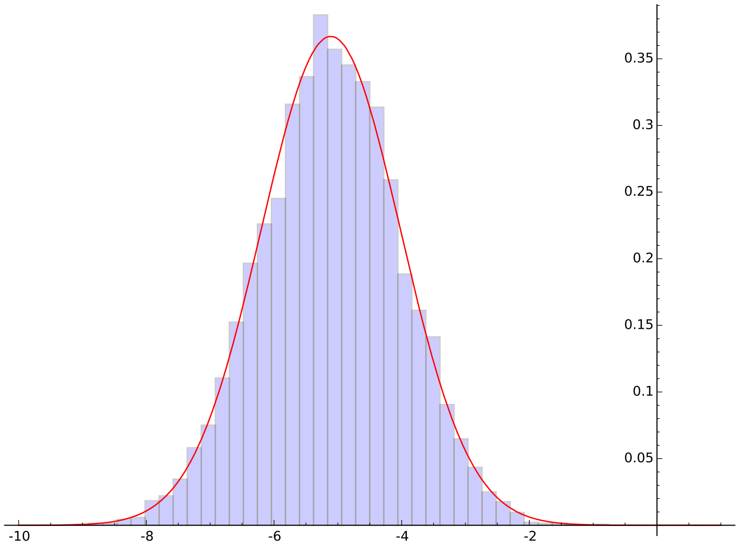


Figure 6. Histogram for $r(h)$, for odd h in (500000,1000000), $3^3||h$. $(\mu, \sigma) = (-5.110585, 1.087463)$.

The exact nature of this "three divisibility bias" is unclear, but inspired by the slow convergence in the Davenport-Heilbronn asymptotic[2]

$$\sum_{\substack{-X<d<0 \\ d \text{ fund. disc.}}} |H(d)[3]| \sim C \cdot X \tag{2.1}$$

(here $H(d)[3]$ denotes the 3-torsion subgroup of $H(d)$) we can slightly adjust $\mathfrak{c}(h)$ to remove most of this bias and obtain a more accurate prediction $\mathrm{pred}'(h)$. (Essentially we examine the exact power of three divisibility

[2] In fact, a negative second order correction to (2.1) of size $X^{5/6}$ was recently obtained by T. Taniguchi and F. Thorne [46], and by M. Bhargava, A. Shankar and J. Tsimmerman [4].

of h and adjust to the data, see Section 6.1 for more details.) With this adjustment, the fluctuations for

$$r'(h) := \frac{\mathcal{F}(h) - \text{pred}'(h)}{\sqrt{\text{pred}'(h)}}$$

(for the full set of odd h) is quite close to a Gaussian.

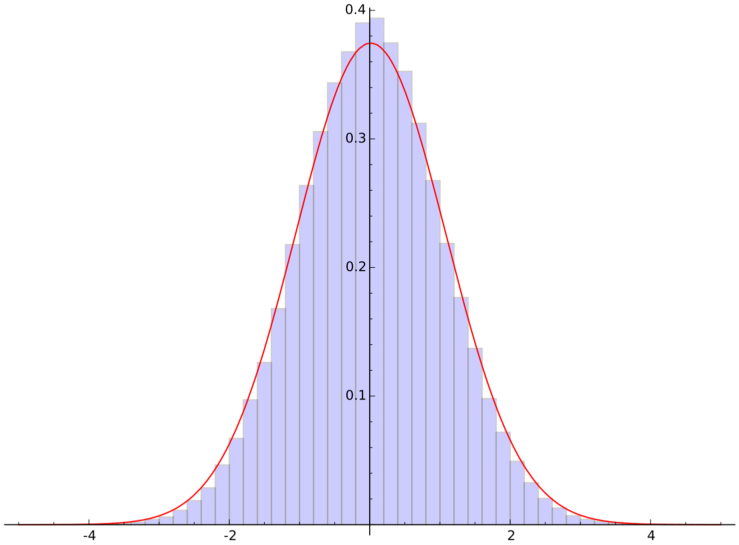


FIGURE 7. Histogram for $r'(h)$, for all odd h in (500000,1000000). $(\mu, \sigma) = (0.013214, 1.065277)$.

However, compared to the fitted Gaussian, the histogram is slightly more peaked, and has less mass in the tails. If we remove integers being divisible by 3^4 this effect is reduced and we get an improved fit to a Gaussian.

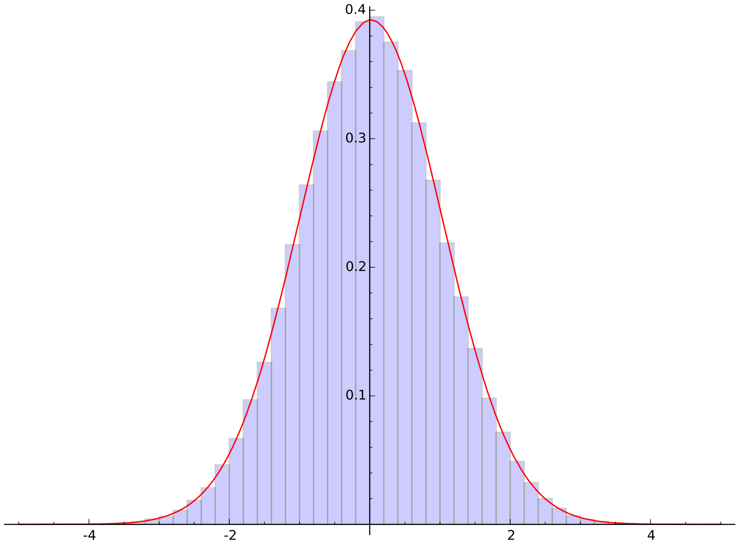


FIGURE 8. Histogram for $r'(h)$, for all odd h in (500000,1000000) and h not divisible by 81. $(\mu, \sigma) = (0.016292, 1.016726)$.

3. Further numerical evidence for Conjecture 1.7

In this section, we present numerical evidence supporting Conjecture 1.7 based on our numerical computation of $\mathcal{F}(G)$, conditional on GRH, for all p-groups G of odd size at most 10^6. (See Section 9 for details regarding the computation.)

3.0.1. *Numerics on $\mathcal{F}(G_\lambda(p))$.* We give in the tables below[3] the value of $\mathcal{F}(G_\lambda(p))$ (conditional on GRH) for each odd prime p and each partition λ of some $n \geq 3$, such that $|G_\lambda(p)| < 10^6$. To be precise: The second column in each table contains all partitions of n for some fixed n, ordered by decreasing cyclicity index $\mathrm{c}(\lambda)$, which itself is given in the leftmost column. The top row contains a list of all primes p such that $p^n < 10^6$, and under each p we list the values of $\mathcal{F}(G_\lambda(p))$ corresponding to the partition λ in the same row. Whenever a partition is omitted from a table, then it is implied that all omitted values of $\mathcal{F}(G_\lambda(p))$ are zero. Groups occuring in rows corresponding to negative cyclicity index ("sporadic groups") are star/bold-marked for emphasis (also see Section 3.0.2.)

$\mathrm{c}(\lambda)$	λ	$p=3$	5	7	11	13	17	19	23	29	31	37	41
3	(3)	88	279	607	1856	2904	5797	7963	12958	24407	29201	46981	62327
1	(2, 1)	5	11	13	19	17	25	22	29	35	26	39	37
−3	(1, 1, 1)	0	0	0	0	0	0	0	0	0	0	0	0

$\mathrm{c}(\lambda)$	λ	$p=43$	47	53	59	61	67	71	73	79	83	89	97
3	(3)	71617	91690	127190	170444	186988	242464	283998	306567	382770	438976	533751	678610
1	(2, 1)	39	29	46	48	57	55	60	66	51	73	66	69
−3	(1, 1, 1)	0	0	0	0	0	0	0	0	0	0	0	0

$\mathrm{c}(\lambda)$	λ	$p=3$	5	7	11	13	17	19	23	29	31
4	(4)	206	1093	3404	16290	29496	77693	116710	233027	548392	701408
2	(3, 1)	19	47	71	146	197	244	343	480	644	779
0	(2, 2)	3	0	0	0	2	1	2	1	0	1
−2	(2, 1, 1)	0	0	0	0	0	0	0	0	0	0
−8	(1, 1, 1, 1)	0	0	0	0	0	0	0	0	0	0

$\mathrm{c}(\lambda)$	λ	$p=3$	5	7	11	13
5	(5)	549	4610	19430	147009	314328
3	(4, 1)	56	218	444	1347	1894
1	(3, 2)	8	5	8	13	9
−1	(3, 1, 1)	0	**1**$*$	0	0	0
−3	(2, 2, 1)	0	0	0	0	0
−7	(2, 1, 1, 1)	0	0	0	0	0
−15	(1, 1, 1, 1, 1)	0	0	0	0	0

$\mathrm{c}(\lambda)$	λ	$p=3$	5	7
6	(6)	1512	19469	116278
4	(5, 1)	177	1024	2887
2	(4, 2)	18	37	58
0	(4, 1, 1)	0	3	0
0	(3, 3)	2	2	3
−2	(3, 2, 1)	0	0	0
−6	(3, 1, 1, 1)	0	0	0
−6	(2, 2, 2)	0	0	0
−8	(2, 2, 1, 1)	0	0	0
−14	(2, 1, 1, 1, 1)	0	0	0
−24	(1, 1, 1, 1, 1, 1)	0	0	0

$\mathrm{c}(\lambda)$	λ	$p=3$	5	7
7	(7)	3881	86038	711865
5	(6, 1)	571	4259	17057
3	(5, 2)	58	177	372
1	(5, 1, 1)	7	7	6
1	(4, 3)	8	11	7
−1	(4, 2, 1)	**1**$*$	0	0
−3	(3, 3, 1)	**1**$*$	0	0
−5	(4, 1, 1, 1)	0	0	0
−5	(3, 2, 2)	0	0	0
−7	(3, 2, 1, 1)	0	0	0
−11	(2, 2, 2, 1)	0	0	0
−13	(3, 1, 1, 1, 1)	0	0	0
−15	(2, 2, 1, 1, 1)	0	0	0
−23	(2, 1, 1, 1, 1, 1)	0	0	0
−35	(1, 1, 1, 1, 1, 1, 1)	0	0	0

$\mathrm{c}(\lambda)$	λ	$p=3$	5
8	(8)	10712	379751
6	(7, 1)	1585	18956
4	(6, 2)	180	719
2	(6, 1, 1)	18	30
2	(5, 3)	15	24
0	(5, 2, 1)	4	1
0	(4, 4)	2	0
−2	(4, 3, 1)	**1**$*$	0
−4	(5, 1, 1, 1)	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$
−48	(1, 1, 1, 1, 1, 1, 1, 1)	0	0

[3] The complete list of all $\mathcal{F}(G_\lambda(p))$ is given in [22], and a complete list of all corresponding discriminants d and groups $H(d)$ is given in [23].

$\mathrm{c}(\lambda)$	λ	$p=3$
9	(9)	28308
7	$(8,1)$	4516
5	$(7,2)$	454
3	$(7,1,1)$	42
3	$(6,3)$	54
1	$(6,2,1)$	10
1	$(5,4)$	4
-1	$(5,3,1)$	**1**$*$
-3	$(6,1,1,1)$	0
$\vdots$	$\vdots$	$\vdots$
-63	$(1,1,1,1,1,1,1,1,1)$	0

$\mathrm{c}(\lambda)$	λ	$p=3$
10	(10)	78657
8	$(9,1)$	12433
6	$(8,2)$	1446
4	$(8,1,1)$	160
4	$(7,3)$	167
2	$(7,2,1)$	16
2	$(6,4)$	14
0	$(6,3,1)$	1
0	$(5,5)$	0
$\vdots$	$\vdots$	$\vdots$
-80	$(1,1,1,1,1,1,1,1,1,1)$	0

$\mathrm{c}(\lambda)$	λ	$p=3$
11	(11)	216520
9	$(10,1)$	35544
7	$(9,2)$	3880
5	$(9,1,1)$	437
5	$(8,3)$	460
3	$(8,2,1)$	58
3	$(7,4)$	49
1	$(7,3,1)$	10
1	$(6,5)$	9
-1	$(8,1,1,1)$	0
-1	$(7,2,2)$	**1**$*$
-1	$(6,4,1)$	**1**$*$
-3	$(7,2,1,1)$	0
$\vdots$	$\vdots$	$\vdots$
-99	$(1,1,1,1,1,1,1,1,1,1,1)$	0

$\mathrm{c}(\lambda)$	λ	$p=3$
12	(12)	603525
10	$(11,1)$	98421
8	$(10,2)$	10988
6	$(10,1,1)$	1291
6	$(9,3)$	1265
4	$(9,2,1)$	220
4	$(8,4)$	133
2	$(8,3,1)$	26
2	$(7,5)$	17
0	$(9,1,1,1)$	2
0	$(8,2,2)$	1
0	$(7,4,1)$	1
0	$(6,6)$	2
-2	$(8,2,1,1)$	**1**$*$
-2	$(7,3,2)$	0
$\vdots$	$\vdots$	$\vdots$
-120	$(1,1,1,1,1,1,1,1,1,1,1,1)$	0

We remark that each vanishing entry in the tables above corresponds to a family of "missing" groups. In particular we see that the group $(\mathbb{Z}/p\mathbb{Z})^3$ does not appear as the class group of a quadratic imaginary field for any prime $2 < p < 100$.

3.0.2. *Sporadic groups in negative cyclicity index case.* As just indicated with bold/star-marks in the tables, each of the groups

$$\frac{\mathbb{Z}}{5^3\mathbb{Z}} \times \left(\frac{\mathbb{Z}}{5\mathbb{Z}}\right)^2, \qquad \frac{\mathbb{Z}}{3^4\mathbb{Z}} \times \frac{\mathbb{Z}}{3^2\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}, \qquad \left(\frac{\mathbb{Z}}{3^3\mathbb{Z}}\right)^2 \times \frac{\mathbb{Z}}{3\mathbb{Z}},$$
$$\frac{\mathbb{Z}}{3^4\mathbb{Z}} \times \frac{\mathbb{Z}}{3^3\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}, \qquad \frac{\mathbb{Z}}{3^5\mathbb{Z}} \times \frac{\mathbb{Z}}{3^3\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}, \qquad \frac{\mathbb{Z}}{3^7\mathbb{Z}} \times \left(\frac{\mathbb{Z}}{3^2\mathbb{Z}}\right)^2,$$
$$\frac{\mathbb{Z}}{3^6\mathbb{Z}} \times \frac{\mathbb{Z}}{3^4\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}, \qquad \frac{\mathbb{Z}}{3^8\mathbb{Z}} \times \frac{\mathbb{Z}}{3^2\mathbb{Z}} \times \left(\frac{\mathbb{Z}}{3\mathbb{Z}}\right)^2$$

occurs exactly once as an imaginary quadratic class group, even though $\mathrm{c}(\lambda) < 0$ for each corresponding partition λ. From the point of view of Conjecture 1.7, these examples may be regarded as "sporadic," since conjecturally they do not belong to an infinite family.

3.0.3. *Zero cyclicity index — the family $\mathcal{F}((\mathbb{Z}/p\mathbb{Z})^2)$.* The case of $\mathrm{c}(\lambda) = 0$ is intermediate in the sense that infinitely many groups in the family should occur, and infinitely many should not. Here the data is quite limited, and we restrict ourselves to the family $G = (\mathbb{Z}/p\mathbb{Z})^2$. The following table contains all odd primes p such that $p^2 < 10^6$, grouped according to the value of $\mathcal{F}((\mathbb{Z}/p\mathbb{Z})^2)$, assuming GRH.

n	All primes $p < 1000$ such that $\mathcal{F}((\mathbb{Z}/p\mathbb{Z})^2) = n$
0	11, 19, 37, 79, 89, 97, 103, 139, 151, 167, 181, 191, 193, 227, 229, 233, 241, 251, 271, 281, 283, 311, 313, 317, 349, 353, 359, 383, 401, 409, 433, 443, 463, 467, 479, 491, 499, 523, 563, 571, 587, 601, 619, 631, 643, 673, 701, 709, 733, 757, 769, 787, 809, 829, 877, 887, 907, 919, 929, 947, 953, 977, 983
1	3, 17, 23, 41, 43, 47, 61, 67, 73, 107, 109, 113, 127, 131, 137, 157, 163, 173, 179, 199, 239, 257, 263, 269, 277, 293, 307, 331, 337, 347, 367, 373, 379, 397, 419, 439, 457, 487, 503, 509, 521, 547, 557, 577, 599, 613, 617, 641, 653, 659, 677, 683, 691, 719, 727, 739, 743, 761, 797, 811, 821, 823, 839, 853, 857, 859, 863, 881, 937, 941, 971, 991, 997
2	5, 7, 29, 31, 53, 59, 71, 83, 101, 197, 211, 223, 389, 431, 449, 461, 569, 593, 607, 647, 661, 827, 883, 911
3	149, 421, 541, 751, 967
4	773
5	13

The limited data seems to support intermediate behaviour.

One may ask how well our prediction of $\mathcal{F}(G)$, using equation (1.2), holds up. The following graph compares the cumulants of the predictions with the observations.

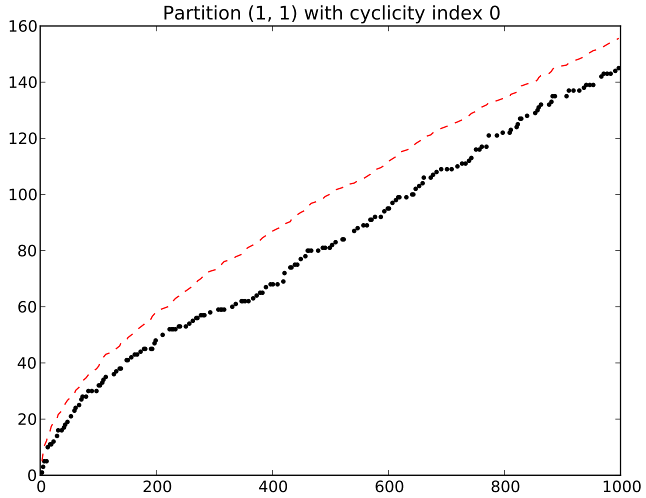


FIGURE 9. *Cumulative* observed values $\sum_{p<x} \mathcal{F}(G_{(1,1)}(p))$ (black dots) compared to *cumulative* predicted values $\sum_{p<x} P(G_{(1,1)}(p)) \operatorname{pred}(p^2)$ (red dashed line), for each $x < 1000$.

4. Preliminaries

In this section, we briefly review relevant background material.

4.1. **Cohen-Lenstra heuristics.** When a finite abelian p-group G occurs in nature, its likelihood of occurrence is often found to be proportional to $1/|\operatorname{Aut}(G)|$. This suggests constructing a discrete probability measure μ on

$$\mathfrak{G}_p := \{\text{isomorphism classes of abelian } p\text{-groups}\}$$

by setting $\mu(\{G\}) := \dfrac{c}{|\operatorname{Aut}(G)|}$ for an appropriate positive constant c, if possible. The following lemma shows that this indeed the case, and is also useful for evaluating c.

Lemma 4.1. *We have that*

$$\sum_{\substack{G\in\mathfrak{G}_p\\|G|=p^n}} \frac{1}{|\operatorname{Aut}(G)|} = \frac{1}{p^n}\prod_{i=1}^{n}\left(1-\frac{1}{p^i}\right)^{-1},$$

$$\sum_{\substack{G\in\mathfrak{G}_p\\|G|\le p^n}} \frac{1}{|\operatorname{Aut}(G)|} = \prod_{i=1}^{n}\left(1-\frac{1}{p^i}\right)^{-1}.$$

Proof. The first equation is [11, Cor 3.8, p. 40]; the second follows from the first by induction on n. □

Let us set

$$\eta_\infty(p) := \prod_{i=1}^{\infty}\left(1-\frac{1}{p^i}\right). \tag{4.1}$$

By taking $n \longrightarrow \infty$ in Lemma 4.1, we see that one must take $c = \eta_\infty(p)$ in order for $\mu(\mathfrak{G}_p) = 1$. In the Cohen-Lenstra model, the probability of G occurring as the p-part of a class group is thus given by

$$\mu(\{G\}) := \frac{\eta_\infty(p)}{|\operatorname{Aut}(G)|}. \tag{4.2}$$

Lemma 4.1 also has the following useful corollary. Here and later in the paper, we will also make use of the notation

$$\begin{aligned}
\mathfrak{D} &:= \{\text{negative fundamental discriminants}\},\\
\mathfrak{D}(x) &:= \{d \in \mathfrak{D} :\ -d \le x\},\\
\mathfrak{D}' &:= \{q \in \mathfrak{D} :\ -q \text{ is prime}\},\\
\mathfrak{D}'(x) &:= \{q \in \mathfrak{D}' :\ -q \le x\}.
\end{aligned}$$

Recall that by genus theory, we have

$$h(d) \text{ is odd} \iff -d \text{ is prime}$$

for $d \in \mathfrak{D}$ with $d < -8$. This observation explains the following notation, wherein P denotes any property of positive odd integers.

$$\operatorname{Prob}(h \text{ satisfies } P :\ h \text{ is an odd class number}) := \lim_{x\to\infty} \frac{\#\{q \in \mathfrak{D}'(x) :\ h(q) \text{ satisfies } P\}}{\#\mathfrak{D}'(x)}. \tag{4.3}$$

Corollary 4.2. *Assuming the Cohen-Lenstra heuristics, for any $n \ge 0$ we have*

$$\operatorname{Prob}(p^n \nmid h :\ h \textit{ is an odd class number}) = \prod_{i=n}^{\infty}\left(1-\frac{1}{p^i}\right)$$

$$\operatorname{Prob}(p^n \parallel h :\ h \textit{ is an odd class number}) = \frac{1}{p^n}\prod_{i=n+1}^{\infty}\left(1-\frac{1}{p^i}\right).$$

Proof. The Cohen-Lenstra heuristics specify that

$$\operatorname{Prob}(p^n \nmid h :\ h \text{ is an odd class number}) = \mu(\{G \in \mathfrak{G}_p : |G| \le p^{n-1}\}).$$

Together with Lemma 4.1, this gives the first equation, and the second equation follows from the first since $\operatorname{Prob}(p^n \parallel h : h \text{ is an odd class number})$ is equal to

$$\operatorname{Prob}(p^n \mid h : h \text{ is an odd class number}) - \operatorname{Prob}(p^{n+1} \mid h : h \text{ is an odd class number}).$$ □

4.2. **The class number formula and special values of L-functions.** Recall the class number formula, which in our context reads

$$L(1,\chi_d)=\frac{\pi h(d)}{\sqrt{|d|}}\qquad (d\in\mathfrak{D}, d<-8), \tag{4.4}$$

where $L(s,\chi_d)=\sum_{n=1}^{\infty}\chi_d(n)n^{-s}$ is the L-function attached to the Kronecker symbol $\chi_d:=\left(\frac{d}{\cdot}\right)$. This formula connects the statistical study of class numbers to that of the special values $L(1,\chi_d)$. Building upon ideas that go back to P.D.T.A. Elliot, A. Granville and K. Soundararajan [16] proved that, on average over $d\in\mathfrak{D}$, $L(1,\chi_d)$ behaves like a random Euler product. More precisely, if $\mathbb{X}(p)$ denotes the random variable defined by

$$\mathbb{X}(p):=\begin{cases}1 & \text{with probability } \frac{p}{2(p+1)}\\ 0 & \text{with probability } \frac{1}{p+1}\\ -1 & \text{with probability } \frac{p}{2(p+1)},\end{cases}$$

and $L(1,\mathbb{X})$ denotes the random Euler product

$$L(1,\mathbb{X}):=\prod_p\left(1-\frac{\mathbb{X}(p)}{p}\right)^{-1},$$

then [16, Theorem 2] (see also [44, p. 4]) implies that, for $|z|\le \log x/(500(\log\log x)^2)$ and $\mathrm{Re}(z)>-1$, we have

$$\sum_{d\in\mathfrak{D}(x)}L(1,\chi_d)^z=|\mathfrak{D}(x)|\cdot\mathbb{E}(L(1,\mathbb{X})^z)+O\left(|\mathfrak{D}(x)|\exp\left(-\frac{\log x}{5\log\log x}\right)\right), \tag{4.5}$$

where $\mathbb{E}$ denotes the expected value. This leads to the average result

$$\sum_{h\le H}\mathcal{F}(h)=\frac{3\zeta(2)}{\zeta(3)}H^2+O\left(H^2(\log H)^{-1/2+\varepsilon}\right), \tag{4.6}$$

for any $\varepsilon>0$ (see [44, Theorem 1]). In the interest of establishing the appropriate constant in Conjecture 1.4, we will next prove Theorem 1.6, which is an analogue of (4.6) averaged over *odd* values of h.

5. The average of $\mathcal{F}(h)$ over odd values of h

In this section we prove Theorem 1.6, that is we develop an asymptotic formula for $\sum_{\substack{h\le H\\ h \text{ odd}}}\mathcal{F}(h)$. By genus theory, the restriction for $h\ge 3$ to be odd is equivalent to the condition that the associated discriminant d be *prime*. As an auxiliary result, we begin by proving the analogue of (4.5) over prime discriminants.

5.1. **The distribution of $L(1,\chi)$ over prime discriminants.** We now prove an asymptotic formula for the general moment of $L(1,\chi_q)$ averaged over $q\in\mathfrak{D}'(x)$. Our proof generally follows the methods used in [16, Theorem 2], but the restriction to prime discriminants demands that we use a different probabilistic model than the model $\mathbb{X}$ introduced earlier. Indeed, $\mathrm{Prob}(\mathbb{X}(p)=0)=1/(p+1)$ corresponds to the probability that a random fundamental discriminant $d\in\mathfrak{D}$ is divisible by the prime p, and one computes

$$\mathrm{Prob}(p\mid d: d\in\mathfrak{D})=\frac{|p\mathbb{Z}/p^2\mathbb{Z}-\{0\}|}{|\mathbb{Z}/p^2\mathbb{Z}-\{0\}|}=\frac{1}{p+1}.$$

On the other hand, the event $p\mid q$ can happen at most once for $q\in\mathfrak{D}'$, and so we replace $\mathbb{X}$ with $\mathbb{Y}$, where we recall that

$$\mathbb{Y}(p):=\begin{cases}1 & \text{with probability } 1/2\\ -1 & \text{with probability } 1/2.\end{cases} \tag{5.1}$$

The corresponding random Euler product is then

$$L(1,\mathbb{Y}):=\prod_p\left(1-\frac{\mathbb{Y}(p)}{p}\right)^{-1}.$$

We will also make use of the following estimate for the remainder term in the Chebotarev density theorem for quadratic fields.

Proposition 5.1. *Assume the Generalized Riemann Hypothesis for Dedekind Zeta functions of quadratic number fields. Then for $d \in \mathbb{N}$ and any real non-principal Dirichlet character χ modulo d, we have*

$$\sum_{\substack{p \leq x \\ \chi(p)=1}} 1 = \frac{1}{2} \operatorname{Li}(x) + O(x^{1/2} \log dx),$$

with an absolute implied constant.

Proof. This is a special case of a theorem of Lagarias-Odlyzko on the error term in the Chebotarev density theorem for general number fields; see [25, Theorem 1.3] and [43, Théorème 2]. □

As an immediate corollary, one deduces the following analogue of the Polya-Vinogradov Theorem, which gives square-root cancellation of characters sums over *prime* values.

Corollary 5.2. *Assume the Generalized Riemann Hypothesis for Dedekind Zeta functions of quadratic number fields. Then for $n \in \mathbb{N}$ which is not a square, we have*

$$\left| \sum_{q \in \mathfrak{D}'(x)} \chi_q(n) \right| \ll x^{1/2} \log(nx),$$

with an absolute implied constant.

The next theorem follows from Corollary 5.2, together with some technical lemmas from [16]. In particular, its proof will utilize several properties of the z-th divisor function $d_z(n)$ for $z \in \mathbb{C}$, which is characterized by the equation

$$\zeta(s)^z = \sum_{n=1}^{\infty} \frac{d_z(n)}{n^s} \qquad (\operatorname{Re}(s) > 1) .$$

Further note that $d_z(n)$ is a multiplicative function, and for prime powers $n = p^a$ we have that

$$d_z(p^a) = \frac{\Gamma(z+a)}{a!\Gamma(z)} = \frac{z(z+1)(z+2)\dots(z+a-1)}{a!} \tag{5.2}$$

Theorem 5.3. *Assume the Generalized Riemann Hypothesis and let $\varepsilon > 0$. Then, uniformly for $|z| \leq \log x/(500(\log\log x)^2)$, we have*

$$\sum_{q \in \mathfrak{D}'(x)} L(1, \chi_q)^z = |\mathfrak{D}'(x)| \cdot \mathbb{E}(L(1, \mathbb{Y})^z) + O_\varepsilon\left(x^{1/2+\varepsilon}\right).$$

Proof. By Lemma 2.3 of [16], for any $Z \in \mathbb{R}$ with $Z \geq \exp\left((\log q)^{10}\right)$ we have

$$L(1, \chi_q)^z = \sum_{n=1}^{\infty} \chi_q(n) \frac{d_z(n)}{n} e^{-n/Z} + O\left(\frac{1}{q}\right).$$

(Note that, since we are assuming GRH, we may ignore any possible exceptional discriminants.) Thus we have

$$\sum_{q \in \mathfrak{D}'(x)} L(1, \chi_q)^z = \sum_{n=1}^{\infty} \frac{d_z(n)}{n} e^{-n/Z} \sum_{q \in \mathfrak{D}'(x)} \chi_q(n) + O(\log\log x). \tag{5.3}$$

The main term in our asymptotic comes from the subsequence $n = m^2$; the other values of n contribute to the remainder term. Indeed, for $n = m^2$, we have

$$\sum_{q \in \mathfrak{D}'(x)} \chi_q(m^2) = |\mathfrak{D}'(x)| + O(\omega(m)),$$

and the contribution of these terms to (5.3) is thus

$$|\mathfrak{D}'(x)| \sum_{m=1}^{\infty} \frac{d_z(m^2)}{m^2} e^{-m^2/Z} + O\left(\log\log x + \sum_{m=1}^{\infty} \frac{|d_z(m^2)\omega(m)|}{m^2} e^{-m^2/Z}\right).$$

Using $\omega(m) \leq d(m)$ together with the bounds

$$\sum_{m=1}^{\infty} \frac{d_z(m^2)d(m)}{m^2} e^{-m^2/Z} \ll \log(|z|+2)^{4|z|+4} \ll_\varepsilon x^\varepsilon$$

and

$$\sum_{m=1}^{\infty} \frac{d_z(m^2)}{m^2}\left(1 - e^{-m^2/Z}\right) \leq \sum_{m=1}^{\infty} \frac{d_{(|z|+1)^2}(m)}{m^2}\left(\frac{m^2}{Z}\right)^{1/4} = \frac{\zeta(3/2)^{(1+|z|)^2}}{Z^{1/4}} \leq \frac{1}{x}$$

(see [16, p. 1014]), one finds that the contribution of the $n = m^2$ terms to (5.3) is thus

$$\begin{aligned}
|\mathfrak{D}'(x)| \sum_{m=1}^{\infty} \frac{d_z(m^2)}{m^2} + O_\varepsilon(x^\varepsilon) &= |\mathfrak{D}'(x)| \prod_p \left(\sum_{j=0}^{\infty} \frac{d_z(p^{2j})}{p^{2j}}\right) + O_\varepsilon(x^\varepsilon) \\
&= |\mathfrak{D}'(x)| \prod_p \left(\sum_{j=0}^{\infty} \binom{-z}{2j} \frac{1}{p^{2j}}\right) + O_\varepsilon(x^\varepsilon) \\
&= |\mathfrak{D}'(x)| \prod_p \frac{1}{2}\left(\left(1+\frac{1}{p}\right)^{-z} + \left(1-\frac{1}{p}\right)^{-z}\right) + O_\varepsilon(x^\varepsilon) \\
&= |\mathfrak{D}'(x)| \cdot \mathbb{E}(L(1,\mathbb{Y})^z) + O_\varepsilon(x^\varepsilon),
\end{aligned}$$

where we have used (5.2) together with the binomial series expansions of $\left(1+\frac{1}{p}\right)^{-z}$ and $\left(1-\frac{1}{p}\right)^{-z}$. In order to handle the terms $n \neq \square$, we begin by inserting the result of Corollary 5.2 into the right-hand side of (5.3), obtaining

$$\begin{aligned}
\left|\sum_{\substack{n=1 \\ n\neq\square}}^{\infty} \frac{d_z(n)}{n} e^{-n/Z} \sum_{q \in \mathfrak{D}'(x)} \chi_q(n)\right| &\ll x^{1/2}\log x \sum_{n=1}^{\infty} \frac{|d_z(n)|}{n} e^{-n/Z} \log n \\
&\ll x^{1/2}\log x \sum_{n=1}^{\infty} \frac{d_{\lceil |z| \rceil}(n)}{n} e^{-n/Z} \log n,
\end{aligned} \tag{5.4}$$

where we have used $|d_z(n)| \leq d_{|z|}(n)$ and $d_{t_1}(n) \leq d_{t_2}(n)$ for $t_1, t_2 \in \mathbb{R}_{>0}$ and $t_1 \leq t_2$. In [16, (2.4), p. 1001] it is observed that $\sum_{n=1}^{\infty} \frac{d_k(n)}{n} e^{-n/Z} \leq (\log 3Z)^k$ for any positive integer k and real number $Z \geq 2$. One may adapt that argument to obtain a similar bound for $\sum_{n=1}^{\infty} \frac{d_k(n)}{n} e^{-n/Z} \log n$ by introducing the function

$$\widetilde{\log}(t) := \begin{cases} 2 & \text{if } t < e^2 \\ \log t & \text{if } t \geq e^2. \end{cases}$$

Note that, for any $a_1, a_2, \ldots, a_k \in \mathbb{N}$ we have

$$\log(a_1 \cdot a_2 \cdot \cdots \cdot a_k) \leq \widetilde{\log}(a_1 \cdot a_2 \cdot \cdots \cdot a_k) \leq \widetilde{\log}(a_1) \cdot \widetilde{\log}(a_2) \cdot \cdots \cdot \widetilde{\log}(a_k).$$

Furthermore, by estimating a discrete sum by a continuous integral we may see that, for Z large enough,

$$\sum_{a=1}^{\infty} \frac{e^{-a/Z}}{a} \widetilde{\log}(a) \ll (\log(e^2 \cdot Z))^2.$$

Using these facts together with the inequality $d_k(n)e^{-n/Z} \leq e^{k/Z} \sum_{a_1 a_2 \ldots a_k = n} e^{-(a_1+a_2+\cdots+a_k)/Z}$, we find that

$$\sum_{n=1}^{\infty} \frac{d_k(n)}{n} e^{-n/Z} \log n \leq \left(e^{1/Z} \sum_{a=1}^{\infty} \frac{e^{-a/Z}}{a} \widetilde{\log}(a)\right)^k \leq (\log(e^2 \cdot Z))^{3k},$$

for Z large enough. Inserting this into (5.4) and taking $Z = \exp\left((\log x)^{10}\right)$, we obtain

$$\begin{aligned}\left|\sum_{\substack{n=1\\ n\neq\square}}^{\infty} \frac{d_z(n)}{n} e^{-n/Z} \sum_{q\in\mathfrak{D}'(x)} \chi_q(n)\right| &\ll x^{1/2}\log x(\log(e^2\cdot Z))^{3\lceil |z|\rceil},\\ &\ll_\varepsilon x^{1/2+\varepsilon}.\end{aligned}$$

This completes the proof of Theorem 5.3. □

5.2. **The proof of Theorem 1.6.** We will largely follow the proof of [44, Theorem 1] with critical modifications in appropriate places; we include the details here for completeness. We make use of the smooth cut-off function

$$\mathfrak{H}_{c,\delta}(x) := \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{x^s}{s}\left(\frac{(1+\delta)^{s+1}-1}{\delta(s+1)}\right) ds,$$

where the parameters $c, \delta > 0$ will be specified soon. For any $c, \delta > 0$ we have

$$\mathfrak{H}_{c,\delta}(x) = \begin{cases} 1 & \text{if } x \geq 1\\ (1+\delta-1/x)/\delta & \text{if } (1+\delta)^{-1}\leq x\leq 1\\ 0 & \text{if } x \leq (1+\delta)^{-1}.\end{cases} \tag{5.5}$$

Just as in [44], by using [16, Theorem 4] , one obtains that

$$\sum_{\substack{h\leq H\\ h \text{ odd}}} \mathcal{F}(h) = \sum_{\substack{q\in\mathfrak{D}'(X)\\ h_q\leq H}} 1 + O_A\left(\frac{H^2}{(\log H)^A}\right) \tag{5.6}$$

for any $A > 0$, where $X := H^2\log\log H$. By the class number formula, (5.6) and (5.5), it follows that

$$\sum_{\substack{h\leq H\\ h \text{ odd}}} \mathcal{F}(h) \leq \sum_{q\in\mathfrak{D}'(X)} \mathfrak{H}_{c,\delta}\left(\frac{\pi H}{\sqrt{q}L(1,\chi_q)}\right) + O_A\left(\frac{H^2}{(\log H)^A}\right) \leq \sum_{\substack{h\leq H(1+\delta)\\ h \text{ odd}}} \mathcal{F}(h).$$

We will now work with the main term in the middle above, which is

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \sum_{q\in\mathfrak{D}'(X)} \left(\frac{\pi}{\sqrt{q}L(1,\chi_q)}\right)^s \frac{H^s}{s}\left(\frac{(1+\delta)^{s+1}-1}{\delta(s+1)}\right) ds. \tag{5.7}$$

We will put $c := 1/\log H$ and $\delta := 1/(\log H)^{1/2}$. We furthermore set $S := \log X/(10^4(\log\log X)^2)$ and decompose the above interval into

$$\int_{|s|\leq S} + \int_{|s|>S}.$$

The second term is easily seen to be

$$\ll \frac{\mathfrak{D}'(X)}{\delta}\int_{|s|>S} \frac{1}{|s(s+1)|}|ds| \ll \frac{H^2}{(\log H)^{3/2-\varepsilon}}.$$

For the integral over $|s| \leq S$, we will use Theorem 5.3 to re-write the integrand in terms of the appropriate moment of $L(1,\mathbb{Y})$ and then reinterpret $\mathfrak{H}_{c,\delta}$ as a smooth cut-off function as in (5.5). First note that the following equation follows immediately from Theorem 5.3 by partial summation:

$$\sum_{q\in\mathfrak{D}'(X)} (\sqrt{q}L(1,\chi_q))^{-s} = \mathbb{E}(L(1,\mathbb{Y})^{-s})\int_1^X t^{-s/2}d\mathfrak{D}'(t) + O_\varepsilon(X^{1/2+\varepsilon}).$$

Thus, (5.7) is equal to

$$\begin{aligned}&\frac{1}{2\pi i}\int_{|s|\leq S} \mathbb{E}(L(1,\mathbb{Y})^{-s})\int_1^X t^{-s/2}d\mathfrak{D}'(t)\frac{(\pi H)^s}{s}\left(\frac{(1+\delta)^{s+1}-1}{\delta(s+1)}\right) ds + O_\varepsilon\left(\frac{H^2}{(\log H)^{3/2-\varepsilon}}\right)\\ =&\mathbb{E}\left(\int_1^X \frac{1}{2\pi i}\int_{|s|\leq S}\left(\frac{\pi H}{\sqrt{t}L(1,\mathbb{Y})}\right)^s \frac{1}{s}\left(\frac{(1+\delta)^{s+1}-1}{\delta(s+1)}\right) ds\, d\mathfrak{D}'(t)\right) + O_\varepsilon\left(\frac{H^2}{(\log H)^{3/2-\varepsilon}}\right)\end{aligned} \tag{5.8}$$

Extending the integral to $\int_{c-i\infty}^{c+i\infty}$ and managing the error, we find that

$$\frac{1}{2\pi i}\int_{|s|\leq S}\left(\frac{\pi H}{\sqrt{t}L(1,\mathbb{Y})}\right)^{s}\frac{1}{s}\left(\frac{(1+\delta)^{s+1}-1}{\delta(s+1)}\right)ds=\mathfrak{H}_{c,\delta}\left(\frac{\pi H}{\sqrt{t}L(1,\mathbb{Y})}\right)+O_{\varepsilon}\left(\frac{L(1,\mathbb{Y})^{-c}}{(\log H)^{3/2-\varepsilon}}\right).$$

Inserting this into (5.8), we find that (5.7) is equal to

$$\begin{aligned}&\mathbb{E}\left(\int_{1}^{\min\left(\frac{\pi^2H^2}{L(1,\mathbb{Y})^2},X\right)}d\mathfrak{D}'(t)+O_{\varepsilon}\left(\frac{H^2}{(\log H)^{3/2-\varepsilon}}(1+L(1,\mathbb{Y})^{-c})\right)\right)\\ =&\frac{1}{2}\mathbb{E}\left(\mathrm{Li}\left(\min\left(\frac{\pi^2H^2}{L(1,\mathbb{Y})^2},X\right)\right)\right)+O_{\varepsilon}\left(\frac{H^2}{(\log H)^{3/2-\varepsilon}}\right).\end{aligned}\tag{5.9}$$

Now using [16, Proposition 1], we find that $\min\left(\frac{\pi^2H^2}{L(1,\mathbb{Y})^2},X\right)=\frac{\pi^2H^2}{L(1,\mathbb{Y})^2}+O_A\left(\frac{H^2}{(\log H)^A}\right)$ for any $A>0$, and so we find that (5.9) becomes

$$\frac{1}{2}\mathbb{E}\left(\mathrm{Li}\left(\frac{\pi^2H^2}{L(1,\mathbb{Y})^2}\right)\right)+O_{\varepsilon}\left(\frac{H^2}{(\log H)^{3/2-\varepsilon}}\right).$$

Finally, using the asymptotic $\mathrm{Li}(x)\sim\dfrac{x}{\log x}$ together with the calculation

$$\begin{aligned}\mathbb{E}(L(1,\mathbb{Y})^{-2})=\prod_p\mathbb{E}\left(\left(1-\frac{\mathbb{Y}(p)}{p}\right)^2\right)&=\prod_p\left(\frac{1}{2}\left(1-\frac{1}{p}\right)^2+\frac{1}{2}\left(1+\frac{1}{p}\right)^2\right)\\ &=\prod_p\left(1-\frac{1}{p^4}\right)\left(1-\frac{1}{p^2}\right)^{-1}=\frac{\zeta(2)}{\zeta(4)}=\frac{15}{\pi^2},\end{aligned}\tag{5.10}$$

the proof of Theorem 1.6 is concluded.

Remark 5.4. Our proof shows that in fact

$$\sum_{\substack{h\leq H\\ h\text{ odd}}}\mathcal{F}(h)=\frac{1}{2}\mathbb{E}\left(\mathrm{Li}\left(\frac{\pi^2H^2}{L(1,\mathbb{Y})^2}\right)\right)+O_{\varepsilon}\left(\frac{H^2}{(\log H)^{3/2-\varepsilon}}\right).$$

We find that the main term in the above expression fits the numerical data much better than the asymptotically equivalent formula given in Theorem 1.6, though it must be stressed that the corrections are of lower order than the error term. In the tables presented in Sections 1 and 9, the number listed under "predicted" refers to the higher order expansion of $\dfrac{\mathfrak{C}}{15}\cdot\mathfrak{c}(h)\cdot h\cdot\mathbb{E}\left(\dfrac{1}{L(1,\mathbb{Y})^2\log(\pi h/L(1,\mathbb{Y}))}\right)$ given in (1.7).

6. Heuristical motivation for Conjecture 1.4

Recall from Remark 5.4 that we have

$$\sum_{\substack{h\leq H\\ h\text{ odd}}}\mathcal{F}(h)\approx\frac{1}{2}\mathbb{E}\left(\mathrm{Li}\left(\frac{\pi^2H^2}{L(1,\mathbb{Y})^2}\right)\right).$$

Denote the right-hand side by $G(H)$. An average order of $\mathcal{F}$ is given by

$$G(h)-G(h-2)\approx 2\frac{d}{dh}G(h)=\mathbb{E}\left(\frac{d}{dh}\mathrm{Li}\left(\frac{\pi^2h^2}{L(1,\mathbb{Y})^2}\right)\right)=$$

$$2\pi^2h\mathbb{E}\left(\frac{1}{L(1,\mathbb{Y})^2\log\left(\pi^2h^2/L(1,\mathbb{Y})^2\right)}\right)=\frac{\pi^2h}{\log(\pi h)}\mathbb{E}\left(\frac{1}{L(1,\mathbb{Y})^2}\frac{1}{1-\frac{\log L(1,\mathbb{Y})}{\log(\pi h)}}\right).$$

With a high probability, we have $|\log L(1,\mathbb{Y})/\log(\pi h)|<1$ for large h, so the above can be approximated with

$$\frac{\pi^2h}{\log(\pi h)}\mathbb{E}\left(\frac{1}{L(1,\mathbb{Y})^2}\left(1+\frac{\log L(1,\mathbb{Y})}{\log(\pi h)}+\frac{\log^2L(1,\mathbb{Y})}{\log^2(\pi h)}+\cdots\right)\right).\tag{6.1}$$

We will approximate this by keeping the first few terms in the innermost parentheses. In this regard, define $c_0 := \mathbb{E}\left(\frac{1}{L(1,\mathbb{Y})^2}\right)$, $c_1 := \frac{1}{c_0}\mathbb{E}\left(\frac{\log L(1,\mathbb{Y})}{L(1,\mathbb{Y})^2}\right)$, $c_2 := \frac{1}{c_0}\mathbb{E}\left(\frac{\log^2 L(1,\mathbb{Y})}{L(1,\mathbb{Y})^2}\right)$, and $c_3 := \frac{1}{c_0}\mathbb{E}\left(\frac{\log^3 L(1,\mathbb{Y})}{L(1,\mathbb{Y})^2}\right)$. Recall from (5.10) that $c_0 = 15/\pi^2$. The constants c_1, c_2 and c_3 may be calculated to arbitrary precision as follows. Write $L_p := 1 - \frac{\mathbb{Y}(p)}{p}$. Then $L(1,\mathbb{Y}) = \prod_p L_p^{-1}$ and $\log L(1,\mathbb{Y}) = -\sum_p \log L_p$. Now

$$\mathbb{E}\left(\frac{\log L(1,\mathbb{Y})}{L(1,\mathbb{Y})^2}\right) = \mathbb{E}\left(-\sum_p \log L_p \prod_r L_r^2\right) = -\sum_p \mathbb{E}\left(L_p^2 \log L_p\right)\prod_{r\neq p}\mathbb{E}\left(L_r^2\right) = -c_0 \sum_p \frac{\mathbb{E}\left(L_p^2 \log L_p\right)}{\mathbb{E}\left(L_p^2\right)} \tag{6.2}$$

where $\mathbb{E}\left(L_p^2\right) = 1 + \frac{1}{p^2}$ and $\mathbb{E}\left(L_p^2 \log L_p\right) = \frac{1}{2}\left((1-\frac{1}{p})^2\log(1-\frac{1}{p}) + (1+\frac{1}{p})^2\log(1+\frac{1}{p})\right)$. Next

$$\mathbb{E}\left(\frac{\log^2 L(1,\mathbb{Y})}{L(1,\mathbb{Y})^2}\right) = \mathbb{E}\left(\sum_{p,q}\log L_p \log L_q \prod_r L_r^2\right) =$$

$$\mathbb{E}\left(\sum_{p\neq q} L_p^2 L_q^2 \log L_p \log L_q \prod_{r\neq p,q} L_r^2 + \sum_p L_p^2(\log L_p)^2 \prod_{r\neq p} L_r^2\right) =$$

$$\sum_{p\neq q}\mathbb{E}\left(L_p^2\log L_p\right)\mathbb{E}\left(L_q^2\log L_q\right)\prod_{r\neq p,q}\mathbb{E}\left(L_r^2\right) + \sum_p \mathbb{E}\left(L_p^2(\log L_p)^2\right)\prod_{r\neq p}\mathbb{E}\left(L_r^2\right) =$$

$$c_0\sum_{p\neq q}\frac{\mathbb{E}\left(L_p^2\log L_p\right)\mathbb{E}\left(L_q^2\log L_q\right)}{\mathbb{E}\left(L_p^2\right)\mathbb{E}\left(L_q^2\right)} + c_0\sum_p\frac{\mathbb{E}\left(L_p^2(\log L_p)^2\right)}{\mathbb{E}\left(L_p^2\right)} =$$

$$c_0\cdot\left(\left(\sum_p\frac{\mathbb{E}\left(L_p^2\log L_p\right)}{\mathbb{E}\left(L_p^2\right)}\right)^2 - \sum_p\left(\frac{\mathbb{E}\left(L_p^2\log L_p\right)}{\mathbb{E}\left(L_p^2\right)}\right)^2 + \sum_p\frac{\mathbb{E}\left(L_p^2(\log L_p)^2\right)}{\mathbb{E}\left(L_p^2\right)}\right) \tag{6.3}$$

where $\mathbb{E}\left(L_p^2(\log L_p)^2\right) = \frac{1}{2}\left((1-\frac{1}{p})^2\log^2(1-\frac{1}{p}) + (1+\frac{1}{p})^2\log^2(1+\frac{1}{p})\right)$. One may similarly show that

$$-\frac{1}{c_0}\mathbb{E}\left(\frac{\log^3 L(1,\mathbb{Y})}{L(1,\mathbb{Y})^2}\right) = \sum_{\substack{p,q,r\\ \text{distinct}}}\frac{\mathbb{E}\left((\log L_p)L_p^2\right)}{\mathbb{E}\left(L_p^2\right)}\frac{\mathbb{E}\left((\log L_q)L_q^2\right)}{\mathbb{E}\left(L_q^2\right)}\frac{\mathbb{E}\left((\log L_r)L_r^2\right)}{\mathbb{E}\left(L_r^2\right)} +$$

$$3\sum_{p\neq r}\frac{\mathbb{E}\left((\log L_p)^2L_p^2\right)}{\mathbb{E}\left(L_p^2\right)}\frac{\mathbb{E}\left((\log L_r)L_r^2\right)}{\mathbb{E}\left(L_r^2\right)} + \sum_p\frac{\mathbb{E}\left((\log L_p)^3L_p^2\right)}{\mathbb{E}\left(L_p^2\right)}. \tag{6.4}$$

Calculating the expressions (6.2), (6.3) and (6.4) with 10^5 prime terms yields[4]

$$c_1 \approx -0.578071, \qquad c_2 \approx +0.604049, \qquad c_3 \approx -0.526259. \tag{6.5}$$

Thus, taking the first four terms of (6.1), an approximation of $\mathcal{F}(h)$ for odd h is

$$\frac{\pi^2 h}{\log(\pi h)}\left(c_0 + \frac{c_0c_1}{\log(\pi h)} + \frac{c_0c_2}{\log^2(\pi h)} + \frac{c_0c_3}{\log^3(\pi h)}\right) = \frac{15h}{\log(\pi h)}\left(1 + \frac{c_1}{\log(\pi h)} + \frac{c_2}{\log^2(\pi h)} + \frac{c_3}{\log^3(\pi h)}\right). \tag{6.6}$$

However, this assumes that each number h occurs as $h(d)$ with equal frequency, which is inconsistent with Corollary 4.2. We thus introduce the correction factor

$$\begin{aligned}\tilde{\mathfrak{c}}(h) := \prod_{\substack{p\geq 3\text{ prime}\\ n\geq 0\\ p^n\| h}}\frac{\mathrm{Prob}(p^n \parallel h' :\ h' \text{ is an odd class number})}{\mathrm{Prob}(p^n \parallel h' :\ h' \text{ is an odd integer})} &= \prod_{\substack{p\geq 3\text{ prime}\\ n\geq 0\\ p^n\| h}}\frac{p^{-n}\prod_{i=n+1}^{\infty}\left(1-\frac{1}{p^i}\right)}{p^{-(n+1)}(p-1)} \\ &= \prod_{\substack{p\geq 3\text{ prime}\\ n\geq 0\\ p^n\| h}}\left(1-\frac{1}{p}\right)^{-1}\prod_{i=n+1}^{\infty}\left(1-\frac{1}{p^i}\right)\end{aligned} \tag{6.7}$$

[4] For techniques to quickly compute these constant with very high precision, see [10, Section 2].

In the above, in addition to using (4.3), we are also using

$$\text{Prob}(h \text{ satisfies } P:\ h \text{ is an odd integer}) := \lim_{x\to\infty} \frac{\#\{h\in\mathbb{N} : h \text{ is odd, } h\le x,\ h \text{ satisfies } P\}}{\#\{h\in\mathbb{N}:\ h \text{ is odd, } h\le x\}}.$$

We emphasize that $n=0$ is allowed in (6.7), and so the expression defining $\tilde{\mathfrak{c}}(h)$ is an *infinite* product. Note that, heuristically at least, we have

$$\sum_{\substack{h\le H\\ h \text{ odd}}} \tilde{\mathfrak{c}}(h) \sim \frac{H}{2}, \qquad (H\longrightarrow\infty). \tag{6.8}$$

Indeed, if $\sum_{\substack{h\le H\\ h \text{ odd}}} \tilde{\mathfrak{c}}(h) \sim B\cdot\frac{H}{2}$, then B has expected value

$$\begin{aligned} B &= \prod_{p \text{ odd}} \sum_{n=0}^{\infty} \text{Prob}(p^n \parallel h:\ h \text{ is an odd integer}) \cdot \frac{\text{Prob}(p^n \parallel h:\ h \text{ is an odd class number})}{\text{Prob}(p^n \parallel h:\ h \text{ is an odd integer})} \\ &= \prod_{p \text{ odd}} \sum_{n=0}^{\infty} \text{Prob}(p^n \parallel h:\ h \text{ is an odd class number}) \\ &= 1. \end{aligned}$$

Noting that

$$\tilde{\mathfrak{c}}(h) = \prod_{\substack{\ell=3\\ \ell \text{ prime}}}^{\infty} \prod_{i=2}^{\infty} \left(1-\frac{1}{\ell^i}\right)\cdot\mathfrak{c}(h) = \frac{\mathfrak{C}}{15}\cdot\mathfrak{c}(h),$$

we get Conjecture 1.4 by multiplying the average order (6.6) with the local correction factor (6.7).

6.1. **Dampening the three divisibility bias.** Given an odd natural number h, let $k\le 11$ and $n\le k-3$ be such that $h\in[3^k,3^{k+1})$ and $3^n \parallel h$. We define the adjustment $\text{pred}'(h)$ by replacing in $\text{pred}(h)$ the factor

$$\text{Prob}(3^n \parallel h':\ h' \text{ is an odd class number}) = 3^{-n}\prod_{i=n+1}^{\infty}\left(1-\frac{1}{3^i}\right)$$

in $\tilde{\mathfrak{c}}(h)$ coming from the Cohen-Lenstra heuristic, by the observed value

$$\text{Prob}(3^n \parallel h':\ h' \text{ is an odd class number} \in [3^k,3^{k+1})) = \sum_{\substack{h'\in[3^k,3^{k+1})\\ h' \text{ odd}\\ 3^n\parallel h'}} \mathcal{F}(h') \Bigg/ \sum_{\substack{h'\in[3^k,3^{k+1})\\ h' \text{ odd}}} \mathcal{F}(h') \tag{6.9}$$

using our computed values of $\mathcal{F}(h)$ (see Section 9).

As mentioned earlier, this three divisibility bias is connected to other recent work: Belabas [3] noted rather slow convergence in the Davenport-Heilbronn asymptotic average of $H(d)$[3]; Roberts [39] later conjectured that this was due to a negative second order term of size $X^{5/6}$ (here the main term is of order X). Robert's conjecture was indepently proved by Bhargava, Shankar and Tsimerman [4], and by Taniguchi and Thorne [46].

7. Heuristical motivation for Conjecture 1.7

We now give heuristics supporting Conjecture 1.7. Let $\lambda=(n_1,n_2,\dots,n_r)$ be a partition of n, so that

$$n_1\ge n_2\ge\cdots\ge n_r\ge 1 \tag{7.1}$$

and $n_1+n_2+\cdots+n_r=n$, and let $G_\lambda(p) := \bigoplus_{i=1}^{r}\mathbb{Z}/p^{n_i}\mathbb{Z}$ be the corresponding abelian group. By the assumption (1.2), the expected value of $\mathcal{F}(G_\lambda(p))$ is

$$\mathcal{F}(G_\lambda(p)) \approx P(G_\lambda(p))\cdot\mathcal{F}(p^n). \tag{7.2}$$

The following proposition evaluates $P(G_\lambda(p))$ explicitly. Let k be the number of distinct parts of λ, and let $m_1, m_2, \ldots, m_k$ be the multiplicity of each distinct part. Thus, (7.1) reads

$$n_1 = \cdots = n_{m_1} > n_{m_1+1} = \cdots = n_{m_1+m_2} > \cdots > n_{\sum_{i=1}^{k-1} m_i+1} = \cdots = n_{\sum_{i=1}^{k} m_i}.$$

Proposition 7.1. *With the notation just given, we have*

$$P(G_\lambda(p)) = p^{\mathrm{c}(\lambda)-n} \cdot \prod_{i=1}^{k}\prod_{j=1}^{m_i}\left(1-\frac{1}{p^j}\right)^{-1}\prod_{i=1}^{n}\left(1-\frac{1}{p^i}\right), \tag{7.3}$$

where $\mathrm{c}(\lambda)$ *is given by* (1.10)*. In particular, as* $p \longrightarrow \infty$*, we have that*

$$P(G_\lambda(p)) \sim p^{\mathrm{c}(\lambda)-n}. \tag{7.4}$$

Proof. The statement follows immediately by combining Lemma 4.1 with the formula

$$|\operatorname{Aut}(G_\lambda(p))| = p^{2n-\mathrm{c}(\lambda)}\prod_{i=1}^{k}\prod_{j=1}^{m_i}\left(1-\frac{1}{p^j}\right).$$

This formula is classical, having appeared in a 1907 paper of A. Ranum [38]. For a more modern exposition, see [20] or [30]. □

Inserting (7.4) together with Conjecture 1.4 into the right-hand side of (7.2), and observing that $\mathfrak{c}(p^n) \longrightarrow 1$ as $p \longrightarrow \infty$, we see that Conjecture 1.7 follows. In the case $\mathrm{c}(\lambda) = 0$ we write

$$\sum_{p\le x}\mathcal{F}(G_\lambda(p)) \sim \sum_{p\le x} P(G_\lambda(p)) \cdot \mathcal{F}(p^n) \sim \sum_{p\le x}\mathfrak{C}\cdot\frac{p^{\mathrm{c}(\lambda)}}{\log(p^n)}$$

and use partial summation.

8. Attainable partitions are very rare

We now prove Theorem 1.9. To this end, let $c_{n,r}$ denote the number of attainable partitions of n into r parts. Work of Sellers ([41],[42]) leads to a generating function for the number of partitions of n which satisfy a certain type of linear inequality amongst their parts:

Theorem 8.1 ([41],[42])**.** *The number of partitions* $\lambda = (n_1, n_2, \ldots, n_r)$ *of* n *into* r *non-negative parts satisfying the inequality* $n_1 \ge \sum_{i=2}^{r} b_i n_i$*, for some non-negative integers* b_i *with* $b_2 > 0$*, has generating function*

$$\frac{1}{(1-x)(1-x^{b_2+1})(1-x^{b_2+b_3+2})(1-x^{b_2+b_3+b_4+3})\cdots(1-x^{b_2+b_3+\cdots+b_r+r-1})}.$$

Applying this result to our context requires a slight modification, and leads to the following generating function for the attainable partitions.

Corollary 8.2. *The generating function* $C_r(x)$ *for the sequence* $c_{n,r}$ *of length-*r *attainable partitions of* n *is given by*

$$C_r(x) = \sum_{n=0}^{\infty} c_{n,r}x^n = \frac{x^{r^2-r}}{(1-x)\prod_{j=2}^{r}(1-x^{j^2-j})}.$$

Proof. First, observe that by definition we require our partitions to be comprised of positive (rather than non-negative) parts. To accommodate this change, we use the easily-verified bijection between partitions of n into r *non-negative* parts satisfying the inequality $b_1 \ge \sum_{i=2}^{r} b_i n_i$ and partitions of $n + \sum_{i=2}^{r} b_i + (r-1)$ into r *positive* parts satisfying the same inequality, given by

$$(n_1, \ldots, n_r) \to (n_1 + \sum_{i=2}^{r} b_i, n_2+1, ..., n_r+1)$$

Thus the analogous generating function to Seller's above for partitions into positive parts is simply a shift of indices away, given by

$$\frac{x^{b_2+b_3+\cdots+b_r+r-1}}{(1-x)(1-x^{b_2+1})(1-x^{b_2+b_3+2})(1-x^{b_2+b_3+b_4+3})\cdots(1-x^{b_2+b_3+\cdots+b_r+r-1})}.$$

Finally, we apply this to attainable partitions, which by definition satisfy an inequality in the form of the theorem, with coefficients $b_i = 2i - 3$. The corollary then follows from the observation

$$j - 1 + \sum_{i=2}^{j} b_i = j - 1 + \sum_{i=2}^{j}(2i-3) = j^2 - j$$

for any $2 \le j \le r$.

□

Basic results about growth rates about coefficients of rational generating functions leads to an asymptotic count of attainable partitions:

Corollary 8.3. *For fixed r, the proportion of length-r partitions of n which are attainable is asymptotically $\frac{1}{(r-1)!}$.*

Proof. We rewrite our expression for $C_r(x)$ to isolate its singularity on the unit circle with the highest multiplicity ($x = 1$ with multiplicity r) and apply the techniques of singularity analysis. Namely, we write

$$\sum_{n=0}^{\infty} c_{n,r} x^n = \frac{1}{(1-x)^r} \cdot \frac{x^{r^2-r+1}}{\prod_{j=2}^{r}(1 + x + x^2 + \cdots + x^{j^2-j-1})} =: \frac{f_r(x)}{(1-x)^r},$$

where here $f_r(x)$ is analytic at $x = 1$. A partial fraction decomposition shows that the asymptotics for the coefficients are governed by this singularity (see, e.g., [15, p. 256]), and we obtain

$$c_{n,r} \sim \frac{f_r(1)n^{r-1}}{(r-1)!} = \frac{n^{r-1}}{(r-1)!\prod_{j=2}^{r}(j^2-j)} = \frac{n^{r-1}}{r!(r-1)!^2}.$$

Similarly, by the well-known generating function

$$\sum_{n=0}^{\infty} p_{n,r} x^n = \frac{x^r}{\prod_{j=1}^{r}(1-x^j)} = \frac{1}{(1-x)^r} \cdot \frac{x^r}{\prod_{j=2}^{r}(1 + x + x^2 + \cdots + x^{j-1})},$$

for $p_{n,r}$, the total number of length-r partitions of n, we conclude that

$$p_{n,r} \sim \frac{n^{r-1}}{r!(r-1)!}.$$

Taking the ratio of these gives

$$\lim_{n\to\infty} \frac{c_{n,r}}{p_{n,r}} = \lim_{n\to\infty} \frac{\frac{n^{r-1}}{r!(r-1)!^2}}{\frac{n^{r-1}}{r!(r-1)!}} = \frac{1}{(r-1)!},$$

proving the result. □

Moving from the fixed rank to the fixed order case, we set

$$c_n = \sum_{r=1}^{n} c_{n,r},$$

the total number of partitions of n which are attainable.

Lemma 8.4. *For fixed n, the numbers $c_{n,r}$ satisfy the recurrence relation*

$$c_{n,r+1} = \sum_{i=0}^{\lfloor \frac{n-2r}{r^2+r} \rfloor} c_{n-2r-i(r^2+r),r}.$$

Proof. From Corollary 8.2 we easily deduce the recurrence relation between the successive generating functions:

$$C_{r+1}(x) = \frac{x^{2r}}{1 - x^{r^2+r}} C_r(x) = (1 + x^{r^2+r} + x^{2(r^2+r)} + \cdots)(x^{2r}C_r(x)),$$

from which the lemma follows by equating coefficients. □

We prove by induction that for fixed $n \geq 1$ we have $c_{n,r} \leq \frac{n^{r-1}}{(r-1)!^2}$ for all r. This is trivial for $r = 1$ since $c_{n,1} = 1$. For the inductive step, the recurrence relation in Lemma 8.4 gives

$$c_{n,r+1} = \sum_{i=0}^{\lfloor \frac{n-2r}{r^2+r} \rfloor} c_{n-2r-i(r^2+r),r} \leq \frac{1}{(r-1)!^2} \sum_{i=0}^{\lfloor \frac{n-2r}{r^2+r} \rfloor} (n-2r-i(r^2+r))^{r-1}.$$

The terms in this sum are positive and decreasing as a function of i, and so we can compare to the integral:

$$\begin{aligned}\sum_{i=0}^{\lfloor \frac{n-2r}{r^2+r} \rfloor} (n-2r-i(r^2+r))^{r-1} &\leq (n-2r)^{r-1} + \int_0^{\lfloor \frac{n-2r}{r^2+r} \rfloor} (n-2r-i(r^2+r))^{r-1}\, di \\ &= n^{r-1} + \frac{n^r}{r(r^2+r)} - \frac{(n-2r-\lfloor \frac{n-2r}{r^2+r} \rfloor (r^2+r))^r}{r(r^2+r)}\end{aligned}$$

Since the latter term is positive and $r^2 + r \leq n$, we can continue

$$c_{n,r+1} \leq \frac{1}{(r-1)!^2} \sum_{i=0}^{\lfloor \frac{n-2r}{r^2+r} \rfloor} (n-2r-i(r^2+r))^{r-1} \leq \frac{1}{(r-1)!^2} \frac{rn^r + n^r}{r(r^2+r)} = \frac{n^r}{r!^2},$$

completing the induction. Now, summing over r gives

$$c_n = \sum_{r=1}^{n} c_{n,r} \leq \sum_{r=1}^{n} \frac{n^{r-1}}{(r-1)!^2} \leq \sum_{r=1}^{\infty} \frac{n^{r-1}}{(r-1)!^2} = I_0(2\sqrt{n}),$$

where $I_0(x)$ denotes the 0-th modified Bessel function of the first kind. By the asymptotic $I_0(x) \sim \frac{e^x}{\sqrt{2\pi x}}$, we can compare the formula for c_n with the famous asymptotic of Hardy-Ramanujan [17], $p_n \sim \frac{e^{\pi\sqrt{2n/3}}}{4n\sqrt{3}}$, for the number of partitions of n. Taking the ratio of the two gives

$$\frac{c_n}{p_n} \ll n^{3/4} e^{(2-\sqrt{\frac{2}{3}}\pi)\sqrt{n}},$$

proving Theorem 1.9.

Remark 8.5. Since $c_{n,1} = 1$ for all $n \geq 1$ (and $c_{0,1} = 0$), Lemma 8.4 provides explicit formulas for the number of attainable partitions of n into a small number of parts. For example,

$$c_{n,2} = \sum_{i=0}^{\lfloor \frac{n-2}{2} \rfloor} c_{n-2-2i,1} = \left\lfloor \frac{n-1}{2} \right\rfloor,$$

agreeing with the easily-checked fact that the partition $[a, b]$ of n is attainable if and only if $a > b$. Less trivially, if we temporarily adopt the simplifying convention that $\lfloor x \rfloor = 0$ for $x < 0$, we have

$$c_{n,3} = \sum_{i=0}^{\lfloor \frac{n-4}{6} \rfloor} c_{n-4-6i,2} = \sum_{i=0}^{\lfloor \frac{n-4}{6} \rfloor} \left\lfloor \frac{n-5-6i}{2} \right\rfloor.$$

This leads to Rademacher-type formulas for computing the exact value of c_n.

9. Description of the computation

With the aid of a supercomputer and assuming GRH, we have computed $\mathcal{F}(h)$ and $\mathcal{F}(G)$ for all odd $h < 10^6$ and all p-groups G of odd size at most 10^6. We have made the computed values available online, see the references [21], [22], [23]. In this section we will describe how this computation was accomplished.

For the correctness of the computation, and to obtain some important speedups, we use GRH in three ways. First, we use a recent result by Lamzouri, Li, and Soundararajan [28] in order to give an upper bound on the negative prime fundamental discriminants $d < 0$ for which $h(d) < 10^6$. More precisely, as already noted, by genus theory, if $-q < -8$ is a fundamental discriminant, then $h(-q)$ is odd precisely when q is prime. Corollary 1.3 in [28] states that under GRH,

$$h(-q) \geq \frac{\pi}{12e^{\gamma}}\sqrt{q}\left(\log\log q - \log 2 + \frac{1}{2} + \frac{1}{\log\log q} + \frac{14\log\log q}{\log q}\right)^{-1} \tag{9.1}$$

if $-q$ is a fundamental discriminant such that $q \geq 10^{10}$. It is easy to verify that the right-hand side above is monotonic for $q \geq 10^{10}$. This implies that if $q \geq 1.1881 \cdot 10^{15}$ then $h(-q) > 10^6$. Thus it suffices to consider only discriminants in $\mathfrak{D}'(1.1881 \cdot 10^{15})$ (recall that $\mathfrak{D}'(x)$ denotes the set of negative fundamental discriminants $-q$ such that $q \leq x$ is prime.)

Secondly, in order to avoid the costly full computation of the class number (especially for $-d > 10^{14}$), we use the Dirichlet class number formula $h(d) = L(1, \chi_d) \cdot \sqrt{|d|}/\pi$ in order to compute a lower bound on $h(d)$ by approximating $L(1, \chi_d)$. Assuming GRH, $L(1, \chi_d)$ is well approximated by a short truncated Euler product; to choose parameters we use some explicit GRH-conditional bounds due to Bach [1] together with a simple, but in practise quite important, improvement (cf. Proposition 9.1.)

Finally, for class groups that are far from cyclic (these are quite rare), we compute the full class group using the procedure `quadclassunit0` in the computer package PARI 2.7.3, an implementation of Buchmann-McCurley's sub-exponential, and GRH-conditional, algorithm (cf. [35, Section 3.4.70].)

9.1. A brief description of the algorithm.

Our computer program iterates over all $d \in \mathfrak{D}'(1.1881 \cdot 10^{15})$ and records for each odd $h < 10^6$ and each noncyclic p-group G, how many times a group of order h or a group isomorphic to G is found, avoiding to compute $h(d)$ or $H(d)$ whenever not necessary (note that if G is a cyclic p-group, then the value of $\mathcal{F}(G)$ can be calculated from the data that we are keeping).

Given a fundamental discriminant $d \in \mathfrak{D}'(1.1881 \cdot 10^{15})$, we begin by calculating an approximation h_{approx} of $h(d)$ together with an explicit error factor E, by setting $h_{\text{approx}} := \frac{\sqrt{|d|}}{\pi}e^{\nu(x_1,d)}$ and $E := e^{\eta(x_1,x_2,d)}$ for suitable x_1, x_2 using Proposition 9.1 below (e.g., towards the end of the discriminant range, it suffices to only consider 7 terms in the truncated Euler product.) If we already at this stage can prove that $h(d) > 10^6$ (that is, if $h_{\text{approx}}/E > 10^6$), then we discard d. This cuts down our search space by roughly a factor of 100, as the lower bound (9.1) is overestimated by roughly this factor in our case.

Otherwise, we compute a candidate h^* for $h(d)$ using Shank's baby-step/giant-step algorithm[5] (specifically, we find an integer h^* near in value to h_{approx} such that g^{h^*} is the identity element for up to three different group elements $g \in H(d)$). (The most time consuming part of the computation consists of discriminants d for which $h(d) < 10^6$; in order to quickly get reasonably good approximations of $h(d)$, we use Proposition 9.1 and take $x_1 = 7919$ and $x_2 = 100000$.) We only compute one such candidate, but in practice, this candidate agrees with the true value of $h(d)$ (assuming GRH) with a failure rate of about $1.5 \cdot 10^{-7}$ for d in our range.

Next, we try to find the exponent of the group by determining the smallest divisor e^* of h^* such that g^{e^*} is the identity element for up to 12 different group elements $g \in H(d)$. We have that e^* divides the order of the group, and if moreover the error factor E is small enough such that h^* is the unique multiple of e^* in the interval $h_{\text{approx}} \cdot [\frac{1}{E}, E]$ then we have proven that $h(d) = h^*$. In practice, this step in our program only catches cyclic groups and groups of the form $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ ($m \geq 3$), but since the majority of the groups $H(d)$ should be of this form[6], our program stops at this step in 99.7% of all cases it is reached.

If any of the above fails (that is, if g^{h^*} was not the identity element for some g or if E was not small enough) or if $h(d)$ was determined to be an odd prime power, then we proceed to compute the structure of the entire class group $H(d)$ using PARI.

Proposition 9.1. *Assume GRH. Let $d < -8$ be a fundamental discriminant and let $x_1 < x_2$ be two integers such that $x_1 \geq 1$ and $x_2 \geq 10^5$. Then*

$$\frac{1}{e^{\eta(x_1,x_2,d)}} \leq \frac{h(d)}{\frac{\sqrt{|d|}}{\pi}e^{\nu(x_1,d)}} \leq e^{\eta(x_1,x_2,d)} \tag{9.2}$$

[5] Using that h is odd, a well known refinement of Shanks' algorithm gives us a speedup factor of $\sqrt{2}$.

[6] We expect the class group to be cyclic more than 97.7% of the time, and class groups containing $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ for prime $q > 5$ are very rare (cf. [11, p. 56].)

where

$$\nu(x_1,d) := \sum_{p\le x_1} -\log\left(1-\frac{(\frac{d}{p})}{p}\right),$$

$$\eta(x_1,x_2,d) := \frac{1.562\log|d| + 0.655\log x_2}{\sqrt{x}_2} + \log\log x_2 + B + \frac{3\log x_2+4}{8\pi\sqrt{x}_2} - \sum_{p\le x_1}\frac{1}{p} + \frac{1}{x_1},$$

and $B := \lim_{x\to\infty}\left(\sum_{p\le x}\frac{1}{p} - \log\log x\right) \approx 0.2614972128\ldots$ *is the prime reciprocal constant.*

Proof. Let χ be the real-valued character $(\frac{d}{\cdot})$ of modulus $|d|>1$. Theorem 9.1 combined with Table 4 in [1] states that under GRH,

$$\left|\log L(1,\chi) - \log\prod_{p<x_2}\frac{1}{1-\frac{\chi(p)}{p}}\right| \le \frac{1.562\log|d| + 0.655\log x_2}{\sqrt{x}_2} \tag{9.3}$$

for any $x_2 \ge 10^5$. By Taylor expansion, we have

$$\begin{aligned}\log\prod_{p<x_2}\frac{1}{1-\frac{\chi(p)}{p}} &= \sum_{p<x_2} -\log\left(1-\frac{\chi(p)}{p}\right)\\ &= \sum_{p\le x_1} -\log\left(1-\frac{\chi(p)}{p}\right) + \sum_{x_1<p<x_2}\sum_{m=1}^{\infty}\frac{1}{m}\left(\frac{\chi(p)}{p}\right)^m.\end{aligned} \tag{9.4}$$

We can bound the terms with $m\ge 2$ by

$$\left|\sum_{x_1<p<x_2}\sum_{m=2}^{\infty}\frac{1}{m}\left(\frac{\chi(p)}{p}\right)^m\right| \le \sum_{x_1<p<x_2}\frac{1}{p^2} \le \int_{x_1}^{\infty}\frac{dt}{t^2} = \frac{1}{x_1}. \tag{9.5}$$

since $\left|\sum_2^\infty \frac{x^m}{m}\right| \le \frac{1}{2}\sum_2^\infty |x|^m = \frac{|x|^2}{2(1-|x|)} \le x^2$ for any $|x|\le\frac{1}{2}$. For $m=1$ we have

$$\left|\sum_{x_1<p<x_2}\frac{\chi(p)}{p}\right| \le \sum_{x_1<p<x_2}\frac{1}{p} < \sum_{p\le x_2}\frac{1}{p} - \sum_{p\le x_1}\frac{1}{p}, \tag{9.6}$$

where the first term on the right-hand side can be bounded using inequality (6.21) in [40], which states that under RH,

$$\sum_{p\le x_2}\frac{1}{p} < \log\log x_2 + B + \frac{3\log x_2+4}{8\pi\sqrt{x}_2} \tag{9.7}$$

for any $x_2 \ge 13.5$.

Combining the inequalities (9.3), (9.4), (9.5), (9.6), (9.7) we obtain

$$|\log L(1,\chi) - \nu(x_1,d)| \le \eta(x_1,x_2,d), \tag{9.8}$$

and the inequality (9.2) follows from taking exponentials and applying the class number formula $h(d) = \frac{\sqrt{|d|}}{\pi}L(1,\chi)$ for $d<-8$. □

9.2. **Computer resources.** Our program comprises 1500 lines of `C++` code. The total time for the computation was 4.5 CPU years, requiring 1 TB of temporary memory storage.

We used the computer package PARI (cf. [35]) to compute the groups $H(d)$ and we used the computer package `primesieve` [47] to iterate through primes.

10. Acknowledgements

P.K. was partially supported by grants from the Göran Gustafsson Foundation for Research in Natural Sciences and Medicine, and the Swedish Research Council (621-2011-5498). S.H. was partially supported by a grant from the Swedish Research Council (621-2011-5498). K.P. was partially supported by Simons Foundation grant # 209266. The computations were performed on resources provided by the Swedish National Infrastructure for Computing (SNIC) at PDC Centre for High Performance Computing (PDC-HPC). We thank the PDC support (Magnus Helmersson, Jonathan Vincent, Radovan Bast, Peter Gille, Jin Gong, Mattias Claesson) for their assistance concerning technical and implementational aspects in making the code run on the PDC-HPC resources.

We would like to thank Andrew Booker, Pete Clark, Henri Cohen, Noam Elkies, Farshid Hajir, Hendrik W. Lenstra, Steve Lester and Peter Sarnak for enlightening conversations on the topic.

References

[1] Eric Bach. Improved approximations for Euler products. In *Number theory (Halifax, NS, 1994)*, volume 15 of *CMS Conf. Proc.*, pages 13–28. Amer. Math. Soc., Providence, RI, 1995.

[2] W. Banks, F. Pappalardi and I. Shparlinski. On group structures realized by elliptic curves over arbitrary finite fields. *Experiment. Math.* **21** (2012), no. 1, 11–25.

[3] K. Belabas. A fast algorithm to compute cubic fields. *Math. Comp.*, 66(219):1213–1237, 1997.

[4] M. Bhargava, A. Shankar, and J. Tsimerman. On the Davenport-Heilbronn theorems and second order terms. *Invent. Math.*, 193(2):439–499, 2013.

[5] A. R. Booker. Quadratic class numbers and character sums. *Math. Comp.*, 75(255):1481–1492 (electronic), 2006.

[6] D. Boyd and H. Kisilevsky. On the exponent of the ideal class groups of complex quadratic fields. *Proc. Amer. Math. Soc.* **31** (1972), 433–436.

[7] D. A. Buell. The last exhaustive computation of class groups of complex quadratic number fields. In *Number theory (Ottawa, ON, 1996)*, volume 19 of *CRM Proc. Lecture Notes*, pages 35–53. Amer. Math. Soc., Providence, RI, 1999.

[8] S. Chowla. An extension of Heilbronn's class number theorem. *Quarterly J. Math.* **5** (1934), 304–307.

[9] L. Claborn. Every abelian group is a class group. *Pacific J. Math.*, 18:219–222, 1966.

[10] H. Cohen. High precision computation of Hardy-Littlewood constants. Preprint, `http://www.math.u-bordeaux1.fr/~cohen/hardylw.dvi`

[11] H. Cohen and H.W. Lenstra. Heuristics on class groups of number fields. Lecture Notes in Mathematics, **1068**, Springer, 1984, pp. 33–62.

[12] G. Cornell. Abhyankar's Lemma and the class group. In *Number theory, Carbondale 1979* (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), 82–88, Lecture Notes in Math., 751, Springer, Berlin, 1979.

[13] C. David and E. Smith. A Cohen-Lenstra phenomenon for elliptic curves. *J. London Math. Soc.* **89** (2014) 24–44.

[14] J. S. Ellenberg and A. Venkatesh. Reflection principles and bounds for class group torsion. *Int. Math. Res. Not. IMRN*, (1):Art. ID rnm002, 18, 2007.

[15] P. Flajolet and R. Sedgewick. Analytic combinatorics. Cambridge University Press, Cambridge, 2009

[16] A. Granville and K. Soundararajan. The distribution of values of $L(1, \chi_d)$. *Geom. and Funct. Anal.* **13** (2003), 992–1028.

[17] G. Hardy and S. Ramanujan. Asymptotic formulae in combinatory analysis. *Proc. London Math. Soc.* **2** (1918) 75–115.

[18] D.R. Heath-Brown. Imaginary quadratic fields with class group exponent 5. *Forum Math.* **20** (2008), 275–283.

[19] H. A. Helfgott and A. Venkatesh. Integral points on elliptic curves and 3-torsion in class groups. *J. Amer. Math. Soc.*, 19(3):527–550 (electronic), 2006.

[20] C. Hillar and D. Rhea. Automorphisms of finite abelian groups. *Amer. Math. Monthly* **114** (2007), 917–923.

[21] S. Holmin, P. Kurlberg. List of $\mathcal{F}(h)$ for all odd $h < 10^6$. Available at `https://people.kth.se/~kurlberg/class_group_data/class_group_orders.txt`

[22] S. Holmin, P. Kurlberg. List of $\mathcal{F}(G)$ for all noncyclic p-groups G of odd order $< 10^6$. Available at `https://people.kth.se/~kurlberg/class_group_data/noncyclic_class_groups.txt`

[23] S. Holmin, P. Kurlberg. List of $(d, H(d))$ for all fundamental discriminants $d < 0$ such that $H(d)$ is a noncyclic p-group of odd order $< 10^6$. Available at `https://people.kth.se/~kurlberg/class_group_data/discriminants_of_noncyclic_groups.txt`

[24] M. J. Jacobson, Jr., S. Ramachandran, and H. C. Williams. Numerical results on class groups of imaginary quadratic fields. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 87–101. Springer, Berlin, 2006.

[25] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem, in A. Frohlich (ed.) *Algebraic Number Fields*, pp. 409–464, Academic Press, 1977.

[26] Y. Lamzouri. On the average of the number of imaginary quadratic fields with a given class number. arXiv:1512.07134.

[27] Y. Lamzouri. The number of imaginary quadratic fields with prime discriminant and class number up to H. arXiv:1701.05267.

[28] Y. Lamzouri, X. Li, and K. Soundararajan. Conditional bounds for the least quadratic non-residue and related problems. *Math. Comp.*, 84(295):2391–2412, 2015.

[29] C. R. Leedham-Green. The class group of Dedekind domains. *Trans. Amer. Math. Soc.*, 163:493–500, 1972.

[30] J. Lengler. The Cohen-Lenstra Heuristic: Methodology and results. *J. Algebra* **323** (2010), 2960–2976.

[31] J. Lengler. The global Cohen-Lenstra Heuristic. *J. Algebra* **357** (2012), 247–269.

[32] A. S. Mosunov and M. J. Jacobson Jr. Unconditional Class Group Tabulation of Imaginary Quadratic Fields to $\Delta < 2^{40}$, arXiv:1502.07953.

[33] J. Oesterlé. Nombres de classes des corps quadratiques imaginaires. *Astérisque*, (121-122):309–323, 1985. Seminar Bourbaki, Vol. 1983/84.

[34] M. Ozaki. Construction of maximal unramified p-extensions with prescribed Galois groups. *Invent. Math.*, 183(3):649–680, 2011.

[35] The PARI Group, Bordeaux. *PARI/GP version* `2.7.3`, 2015. Available at `http://pari.math.u-bordeaux.fr/pub/pari/unix/pari-2.7.3.tar.gz`.

[36] M. Perret. On the ideal class group problem for global fields. *J. Number Theory*, 77(1):27–35, 1999.

[37] L. B. Pierce. A bound for the 3-part of class numbers of quadratic fields by means of the square sieve. *Forum Math.*, 18(4):677–698, 2006.

[38] A. Ranum. The group of classes of congruent matrices with application to the group of isomorphisms of any abelian group. *Trans. Amer. Math. Soc.* **8** (1907), 71–91.

[39] D. P. Roberts. Density of cubic field discriminants. *Math. Comp.*, 70(236):1699–1705 (electronic), 2001.

[40] Lowell Schoenfeld. Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II. *Math. Comp.*, 30(134):337–360, 1976.

[41] James A. Sellers. Extending a recent result of Santos on partitions into odd parts. *Integers* **3:A4**, 5 pp. (electronic), 2003.

[42] James A. Sellers. Corrigendum to: "Extending a recent result of Santos on partitions into odd parts". *Integers* **4:A8**, 1 pp. (electronic), 2004.

[43] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Publ. Math. I. H. E. S.* **54** (1981), 123–201.

[44] K. Soundararajan. The number of imaginary quadratic fields with a given class number. *Hardy-Ramanujan J.* **30** (2007), 13–18.

[45] A. V. Sutherland. *Order computations in generic groups.* ProQuest LLC, Ann Arbor, MI, 2007. Thesis (Ph.D.)–Massachusetts Institute of Technology.

[46] T. Taniguchi and F. Thorne. Secondary terms in counting functions for cubic fields. *Duke Math. J.*, **162** (2013), 2451–2508.

[47] K. Walisch. `primesieve`. Fast C/C++ prime number generator. Available at `http://primesieve.org/`.

[48] M. Watkins. Class numbers of imaginary quadratic fields. *Math. Comp.* **73** (2003), 907–938.

[49] P. Weinberger. Exponents of the class groups of complex quadratic fields. *Acta Arith.* **22** (1973), 117–124.

[50] O. Yahagi. Construction of number fields with prescribed l-class groups. *Tokyo J. Math.* **1** (1978), no. 2, 275–283.

[51] Y. Yamamoto. On unramified Galois extensions of quadratic number fields, *Osaka J. Math.* **7** (1970), 57–76.

(Samuel Holmin)

- Department of Mathematics, KTH, SE-10044, Stockholm, Sweden.

E-mail address, Samuel Holmin: `holmin@kth.se`

(Nathan Jones, corresponding author)

- Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 322 Science and Engineering Offices (M/C 249), 851 S. Morgan Street, Chicago, IL 60607-7045, USA.

E-mail address, Nathan Jones: `ncjones@uic.edu`

(Pär Kurlberg)

- Department of Mathematics, KTH, SE-10044, Stockholm, Sweden.

E-mail address, Pär Kurlberg: `kurlberg@math.kth.se`

(Cam McLeman)

- University of Michigan – Flint, Mathematics Department, 402 Murchie Science Building, Flint, MI 48502-1950, USA.

E-mail address, Cam McLeman: `mclemanc@umflint.edu`

(Kathleen L. Petersen)

- Department of Mathematics, Florida State University, 208 Love Building, 1017 Academic Way, Tallahassee, FL 32306-4510, USA.

E-mail address, Kathleen L. Petersen: `petersen@math.fsu.edu`