ON THE AVERAGE NUMBER OF OCTAHEDRAL NEWFORMS OF PRIME LEVEL

MANJUL BHARGAVA AND EKNATH GHATE

Abstract. We show that, on average, the number of octahedral newforms of prime level is bounded by a constant.

1. Introduction

This paper is concerned with counting holomorphic cuspidal newforms of weight 1. To each such form f, Deligne and Serre associate an odd irreducible Galois representation $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$, whose image in $\mathrm{PGL}_2(\mathbb{C})$ is, by a standard classification, either

- a dihedral group, or,
- A_4, S_4 or A_5.

In the last three cases the form f is said to be of tetrahedral, octahedral, or icosahedral type, respectively. Extensive numerical computations [Fre94] suggest that these forms occur extremely rarely, and they have been traditionally labelled as *exotic*. Forms of prime level have in particular long held a special place in the literature [Ser77], [Duk95]. It is a standard conjecture that

Conjecture 1.1. *For any $\epsilon > 0$, the number of exotic newforms of prime level N is $O(N^{\epsilon})$, where the implied constant depends only on ϵ.*

It appears that this conjecture has its origins in a remark of Serre [Ser77, p. 259], where it was observed that the number of exotic forms of prime level $N \equiv 3 \mod 4$ is $O(N^{\alpha})$, with $\alpha = 1$. Serre asks whether this assertion continues to hold with $\alpha < 1$, or even $\alpha < 1/2$.

Subsequent articles have made considerable progress towards Conjecture 1.1. For instance in the octahedral case, Duke [Duk95], Wong [Won99], Michel-Venkatesh [MV02], Ganguly [Gan06], Ellenberg [Ell03], and Klüners [Klu06] have established bounds of $O(N^{7/8+\epsilon})$, $O(N^{5/6+\epsilon})$, $O(N^{4/5+\epsilon})$, $O(N^{3/4+\epsilon})$, $O(N^{2/3+\epsilon})$ on average, and $O(N^{1/2+\epsilon})$, respectively. Many of these papers obtain bounds in the tetrahedral and icosahedral cases, and some of these papers consider certain non-prime levels as well.

Date: January 30, 2009.

It is known that any exotic weight one form of prime level must be either octahedral or icosahedral. The goal of this paper is to prove Conjecture 1.1 *on average* for octahedral newforms of prime level. In fact we prove something much stronger, namely, that the number of such forms is on average bounded by an absolute constant. Indeed, we prove:

Theorem 1.2. *Let*

$$N_{\mathrm{oct}}^{\mathrm{prime}}(X) = \big|\{\text{octahedral cuspidal newforms } f \text{ having prime level } < X\}\big|.$$

Then $N_{\mathrm{oct}}^{\mathrm{prime}}(X) = O(X/\log X)$.

Since, by the prime number theorem, the number of primes up to X is asymptotic to $X/\log X$, it follows that on average the number of octahedral cuspidal newforms of prime level N is $O(1) = O(N^\epsilon)$, for any $\epsilon > 0$.

Our methods also allow us to prove Conjecture 1.1, on average, for a much larger class of conductors. Say that a number is *good* if it is either prime or if it is a product of odd primes which are congruent to 2 mod 3. Then we have:

Theorem 1.3. *Let*

$$N_{\mathrm{oct}}^{\mathrm{good}}(X) = \big|\{\text{octahedral cuspidal newforms } f \text{ having good level } < X\}\big|.$$

Then $N_{\mathrm{oct}}^{\mathrm{good}}(X) = O(X^{1+\epsilon})$.

Thus on average the number of octahedral forms of good level N is again $O(N^\epsilon)$.

The proofs of Theorems 1.2 and 1.3 involve relating octahedral newforms to the 2-torsion in class groups of cubic fields, keeping track of the somewhat subtle relationship between the discriminant of the cubic field and the level of the form. A suitable adaptation of the result in [Bha05], which computes the average number of 2-torsion elements in class groups of cubic fields, together with an appropriate sieve in the case of prime levels, is then utilized to prove Theorems 1.2 and 1.3.

Here is a more detailed overview of the paper. In Section 2 we recall the standard dictionary between exotic forms, their associated two-dimensional complex Galois representations, and certain quartic or quintic number fields. In Section 3 we recall some facts about projective Galois representations. In Section 4 we provide tables which compare the exponents of primes occurring in the support of the conductor of a minimal exotic form and the discriminant of the corresponding quartic or quintic number field. These tables contain the key raw data one needs in going back and forth between minimal exotic forms and number fields. In Section 5 we establish a bound on the number of twists that preserve the level of a minimal form. In Section 6 we begin counting minimal octahedral forms, using the tables in Section 4, and the results of [Bha05]. We prove Theorem 6.2, which is a stronger form of Theorem 1.3. In Section 7 we refine the main result of [Bha05] on the asymptotic enumeration of quartic fields from all discriminants to prime discriminants. This involves proving certain equidistribution results for pairs of ternary quadratic forms mod p, and then using a prime sieve. This allows us to obtain Theorem 1.2 in Section 8.

2. Artin conjecture

For brevity we use the term *newform* to refer to a normalized newform which is a common eigenform for all the Hecke operators. For counting purposes the following result will be useful.

Theorem 2.1. *The following sets are naturally in bijection:*

(1) $\{$ *octahedral cuspidal newforms of weight* 1*, up to twist* $\}$

(2) $\{$ *isomorphism classes of odd representations* $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ *with projective image* S_4*, up to twist* $\}$

(3) $\{$ *isomorphism classes of projective representations* $\tilde{\rho} : G_{\mathbb{Q}} \to \mathrm{PGL}_2(\mathbb{C})$ *with image* S_4*, such that* $\tilde{\rho}(c) \neq 1$ $\}$

(4) $\{$ *isomorphism classes of non-real quartic number fields* K*, with Galois closure* E *having Galois group* $\mathrm{Gal}(E/\mathbb{Q}) = S_4$ $\}$.

Proof. This is well known so we only make some brief remarks here (see, for example, Serre's informative article [Ser77] for more details). That (1) is in bijection with (2) holds even without the qualification *up to twist* (by a Dirichlet character). The theorem of Deligne and Serre referred to in the introduction induces an injective map from the set (1) to the set (2). The Artin conjecture, which in the octahedral case is a theorem of Langlands and Tunnell, says that this map is a bijection. Moreover, the level of a newform f matches with the conductor of the corresponding representation ρ_f. That (2) is in bijection with (3) follows from the fact that obstructions to lifting projective representations lie in $\mathrm{H}^2(G_{\mathbb{Q}}, \mathbb{C}^\times)$, which vanishes by a theorem of Tate. The oddness of ρ is equivalent to the condition $\tilde{\rho}(c) \neq 1$, where c is complex conjugation. Finally the sets (3) and (4) above are in bijection via an embedding of S_4 in $\mathrm{PGL}_2(\mathbb{C})$, noting that in the octahedral case any two such embeddings are conjugate. The condition on complex conjugation is equivalent to the fact that K (equivalently E) is not a totally real number field. □

Similar theorems hold in the tetrahedral and icosahedral cases. The Artin conjecture in the tetrahedral case was established earlier by Langlands. Several cases of the Artin conjecture in the icosahedral case were established by Buzzard, Dickinson, Shepherd-Barron and Taylor. Recently Khare and Wintenberger, and Kisin, have announced a proof of Serre's modularity conjecture. Since Khare had earlier shown that Serre's conjecture implies (all cases of) the Artin conjecture for odd representations, this would establish the remaining open icosahedral cases of the Artin conjecture as well.

3. Projective Galois representations

We now recall some results of Tate concerning two-dimensional projective Galois representations which were written down by Serre [Ser77].

Theorem 3.1 (Tate, cf. [Ser77, Thm. 5])**.** *Let $\tilde{\rho} : G_{\mathbb{Q}} \to \mathrm{PGL}_2(\mathbb{C})$ be a projective representation. For each prime p, let ρ'_p be a lift of $\tilde{\rho}|_{D_p}$. Suppose that $\rho'_p|_{I_p} = 1$ for almost all p. Then there exists a unique lift $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ of $\tilde{\rho}$ such that $\rho|_{I_p} = \rho'_p|_{I_p}$ for all p.*

Definition 3.2. Let $\tilde{\rho} : G_{\mathbb{Q}} \to \mathrm{PGL}_2(\mathbb{C})$ be a projective representation. The *conductor* of $\tilde{\rho}$ is defined to be the positive integer

$$N = \prod_p p^{m(p)}$$

where $m(p)$ is the least integer such that $\tilde{\rho}|_{D_p}$ has a lifting of conductor $p^{m(p)}$.

Since the conductor of a (linear) representation is determined by its restriction to (all) inertia subgroups, it follows from the theorem of Tate above that if the conductor of $\tilde{\rho}$ is N, then there is a lifting ρ of $\tilde{\rho}$ of conductor N. Moreover every lift ρ has conductor a multiple of N.

A lifting of $\tilde{\rho}$ (respectively $\tilde{\rho}|_{D_p}$) is reducible if and only if $\tilde{\rho}(G_{\mathbb{Q}})$ (respectively $\tilde{\rho}(D_p)$) is a cyclic group. The following proposition gives information about the exponents $m(p)$ appearing in the conductor of $\tilde{\rho}$, in various cases.

Proposition 3.3 (cf. [Ser77, §6.3, §8.1])**.** *Let $\tilde{\rho} : G_{\mathbb{Q}} \to \mathrm{PGL}_2(\mathbb{C})$ be a projective representation.*

1. *If $\tilde{\rho}$ is unramified at p, then $\tilde{\rho}(D_p)$ is a cyclic group, and $m(p) = 0$.*
2. *If $\tilde{\rho}$ is ramified at p, but only tamely ramified at p (that is, $\tilde{\rho}(I_{\mathrm{wild}}) = 1$), then $\tilde{\rho}(D_p)$ is cyclic or dihedral. In the former case $m(p) = 1$, and in the latter case $m(p) = 2$.*
3. *Moreover, if $i_p = |\tilde{\rho}(I_p)|$ is still prime to p, and $i_p \geq 3$, then $m(p) = 1$ if and only if $i_p \mid (p-1)$.*
4. *If $\tilde{\rho}(I_{\mathrm{wild}}) \neq 1$ and $p > 2$, then $\tilde{\rho}(D_p)$ is still cyclic or dihedral, but if $p = 2$, then $\tilde{\rho}(D_p)$ can also be A_4 or S_4.*

The exponents $m(p)$ in the wildly ramified cases have been tabulated by Buhler and Zink (cf. pages 10–26 of Kiming's article in [Fre94]). In any case, these exponents are bounded, which is all we need below.

4. Conductor vs Discriminant

In this section we compare the conductor of a projective Galois representation with the discriminant of the associated quartic or quintic number field. While these quantities have the same primes p in their supports, the exact power of p dividing each may vary considerably. This leads to complications when one counts forms by conductor by appealing to counting results for number fields (which usually count by discriminant).

Let $\tilde{\rho} : G_{\mathbb{Q}} \to \mathrm{PGL}_2(\mathbb{C})$ be an irreducible projective representation such that the image of $\tilde{\rho}$ is either A_4, S_4, or A_5. Let E be the field cut out by $\tilde{\rho}$, and assume that $K \subset E$ is either a quartic field or a quintic field whose Galois closure is E. So $\mathrm{Gal}(E/\mathbb{Q}) = A_4$, S_4, or A_5. Recall that these cases are called the tetrahedral, octahedral and icosahedral cases respectively.

For a number field F, if p factors as $P_1^{e_1} P_2^{e_2} \cdots P_r^{e_r}$ in the ring of integers $\mathcal{O}_F$ of F, then we say that p has *ramification type* $f_1^{e_1} f_2^{e_2} \cdots f_r^{e_r}$ *in* F, where f_i denotes the cardinality of the residue field $\mathcal{O}_F/P_i$ of P_i. As is customary, we drop the exponent e_i when $e_i = 1$. If $p \geq 5$ ($p \geq 7$ in the icosahedral case), then p is (at most) tamely ramified in E and K, and the image of I_p under $\tilde{\rho}$ is cyclic. Also, by part (2) of Proposition 3.3, the image of D_p under $\tilde{\rho}$ is either cyclic or dihedral. In the tables below we list all possible non-trivial ramification types for such p in E and K, corresponding to all possible choices of the inertia and decomposition subgroups in $\mathrm{Gal}(E/\mathbb{Q})$. We write $V_4 \subset S_4$ for the Klein 4-group and $\mathrm{Dih}_n \subset S_n$ for a dihedral group with $2n$ elements. For each ramification type we list the power of p appearing in $\mathrm{Disc}(K)$, the discriminant of K, and the power of p appearing in the conductor of $\tilde{\rho}$ using part (2) of Proposition 3.3. In the last column we list any congruence conditions on p which are forced by part (3) of Proposition 3.3.

Table 1: Tetrahedral Case

I_p	D_p	Ram in E	Ram in K	Disc(K)	Cond($\tilde{\rho}$)	$p \equiv$
$\langle(12)(34)\rangle$	I_p	$\underbrace{1^2 1^2 \cdots 1^2}_{6}$	$1^2 1^2$	p^2	p	
$\langle(12)(34)\rangle$	V_4	$2^2 2^2 2^2$	2^2	p^2	p^2	
$\langle(123)\rangle$	I_p	$1^3 1^3 1^3$	$1^3 1$	p^2	p	$1 \mod 3$

Table 2: Octahedral Case

I_p	D_p	Ram in E	Ram in K	Disc(K)	Cond$(\tilde{\rho})$	$p \equiv$
$\langle(12)\rangle$	I_p	$\underbrace{1^2 1^2 \cdots 1^2}_{12}$	$1^2 11$	p	p	
$\langle(12)\rangle$	$\langle(12),(34)\rangle$	$\underbrace{2^2 2^2 \cdots 2^2}_{6}$	$1^2 2$	p	p^2	
$\langle(12)(34)\rangle$	I_p	$\underbrace{1^2 1^2 \cdots 1^2}_{12}$	$1^2 1^2$	p^2	p	
$\langle(13)(24)\rangle$	$\langle(1234)\rangle$	$\underbrace{2^2 2^2 \cdots 2^2}_{6}$	2^2	p^2	p	
$\langle(12)(34)\rangle$	V_4	$\underbrace{2^2 2^2 \cdots 2^2}_{6}$	2^2	p^2	p^2	
$\langle(12)(34)\rangle$	$\langle(12),(34)\rangle$	$\underbrace{2^2 2^2 \cdots 2^2}_{6}$	$1^2 1^2$	p^2	p^2	
$\langle(123)\rangle$	I_p	$\underbrace{1^3 1^3 \cdots 1^3}_{8}$	$1^3 1$	p^2	p	$1 \mod 3$
$\langle(123)\rangle$	S_3	$2^3 2^3 2^3 2^3$	$1^3 1$	p^2	p^2	$2 \mod 3$
$\langle(1234)\rangle$	I_p	$\underbrace{1^4 1^4 \cdots 1^4}_{6}$	1^4	p^3	p	$1 \mod 4$
$\langle(1234)\rangle$	Dih_4	$2^4 2^4 2^4$	1^4	p^3	p^2	$3 \mod 4$

Table 3: Icosahedral Case

I_p	D_p	Ram in E	Ram in K	Disc(K)	Cond$(\tilde{\rho})$	$p \equiv$
$\langle(12)(34)\rangle$	I_p	$\underbrace{1^2 1^2 \cdots 1^2}_{30}$	$1^2 1^2 1$	p^2	p	
$\langle(12)(34)\rangle$	V_4	$\underbrace{2^2 2^2 \cdots 2^2}_{15}$	$2^2 1$	p^2	p^2	
$\langle(123)\rangle$	I_p	$\underbrace{1^3 1^3 \cdots 1^3}_{20}$	$1^3 11$	p^2	p	$1 \mod 3$
$\langle(12345)\rangle$	I_p	$\underbrace{1^5 1^5 \cdots 1^5}_{12}$	1^5	p^4	p	$1 \mod 5$
$\langle(12345)\rangle$	Dih_5	$\underbrace{2^5 2^5 \cdots 2^5}_{6}$	1^5	p^4	p^2	$2,3,4 \mod 5$

5. Minimal Level

Eventually, we will restrict to counting minimal cuspidal newforms. This class of forms includes forms of prime level. Recall that a cuspidal newform is said to be *minimal* if its level is minimal amongst all its twists by Dirichlet characters of arbitrary conductor. That is, f is minimal if (the newform attached to) $f \otimes \chi$ does not have strictly smaller conductor for any χ. Since two forms give the same projective representation if and only if they are twists of each other, it follows from the remarks made in Section 3 that the level of a minimal form is the conductor of the associated projective representation.

Twisting a minimal form generally tends to raise its level. However, it is possible for the twist of a minimal form to be minimal, i.e., of the same level. For instance, if $S_1(N, \epsilon)$ denotes the space of cusp forms of level N and nebentypus ϵ, and ϵ is real, then the newform attached to $f \otimes \epsilon$ is just $\bar{f}$, the form obtained by taking the complex conjugates of the Fourier coefficients of f, and this form clearly lies in the same space. Since we will count (minimal) forms by counting their *projective* Galois representations, this phenomenon of 'level stabilization under twist' has potential to cause problems; *a priori* there may be many minimal forms giving rise to the same projective Galois representation.

However, in this section we show that only finitely many twists of a form of minimal level can be minimal of the same level; moreover, the number of such twists is bounded by a constant that depends only on the *number* of primes dividing the minimal level. We begin by proving the following proposition (see also [Ell03, Lemma 1]):[1]

Proposition 5.1. *Let $f \in S_1(N, \epsilon)$ be an exotic cuspidal newform of minimal level N. Assume that ρ_f is tamely ramified at each prime $p|N$. Then there exists a positive integer M_0, independent of N, such that $\epsilon^{M_0} = 1$. In fact $M_0 = 6$, 12 and 30 in the tetrahedral, octahedral and icosahedral cases, respectively.*

Proof. Note that ϵ has conductor dividing N. Decompose $\epsilon = \prod_{p|N} \epsilon_p$ where ϵ_p is the p-part of ϵ. It is enough to show that $\epsilon_p^{M_0} = 1$, for each p. To do this, note that since ρ_f is tamely ramified at p, the restriction of ρ_f to I_p, $\rho_f|_{I_p}$, has cyclic image in $\mathrm{GL}_2(\mathbb{C})$. So $\rho_f|_{I_p}$ is reducible, and therefore semi-simple since we are working over the complex numbers. Say that

$$\rho_f|_{I_p} \sim \begin{pmatrix} \psi_1 & 0 \\ 0 & \psi_2 \end{pmatrix}$$

where ψ_1, and ψ_2 are characters of I_p. Since f has minimal level, we have $\psi_1 \neq \psi_2$; otherwise, thinking of ψ_1 as a character of $G_{\mathbb{Q}}$, the Galois representation attached to the

[1] Proposition 5.1 and Corollary 5.2 may not hold when N is not square-free: see Errata

twisted form $f \otimes \psi_1^{-1}$ would be trivial on inertia and so would have strictly smaller level (at p). If follows that the image of $\rho_f|_{I_p}$ injects into $\mathrm{PGL}_2(\mathbb{C})$. Since f is exotic, the image is a (cyclic) subgroup of A_4, S_4, or A_5. All such subgroups have order ≤ 5, the possible orders being $1, 2, 3$ for A_4, $1, 2, 3, 4$ for S_4, and $1, 2, 3, 5$ for A_5. It follows that the characters ψ_1 and ψ_2 are killed by $M_0 = 6$, 12, and 30 respectively. On the other hand since $\det(\rho_f) = \epsilon$, we have $\det(\rho_f|_{I_p}) = \epsilon_p = \psi_1\psi_2$. Thus $\epsilon_p^{M_0} = 1$. □

We are now able to conclude what we want. As is usual, we use $\omega(N)$ to denote the number of distinct prime divisors of N.

Corollary 5.2. *Let $f \in S_1(N, \epsilon)$ be an exotic newform of minimal level N. Then there are only finitely many Dirichlet characters χ such that $f \otimes \chi$ is minimal of level N, and the number of such χ is bounded by $M^{\omega(N)}$, for some absolute constant $M \geq 1$.*

Proof. Assume momentarily that N is prime to 6 (prime to 30 in the icosahedral case). Suppose $f \otimes \chi$ also has level N. Then both ρ_f and $\rho_f \otimes \chi$ are tamely ramified. Now $f \otimes \chi$ has nebentypus $\epsilon\chi^2$. By the proposition, both ϵ and $\epsilon\chi^2$ are killed by M_0, so $\chi^{2M_0} = 1$. Now the support of the conductor of χ is a finite set, contained in the support of N, since otherwise the level of the twisted form would contain new primes. It follows that there are only finitely many possibilities for χ, and that this number is bounded by $(2M_0)^{\omega(N)}$. Even if N is not relatively prime to 6 (or 30 in the icosahedral case), the number of χ preserving a given minimal level N is still bounded. For the tame part of N we argue as above. For the wild part of N we note that the exponents of 2 and 3 (and 5 in the icosahedral case) in N, equivalently the exponents $m(2)$ and $m(3)$ (and $m(5)$ in the icosahedral case) appearing in the conductor of the underlying projective representation are bounded. Thus the number of permissible 2 and 3-parts of χ (and 5-part of χ in the icosahedral case) which will preserve these bounds, must be bounded as well, say by M_2, M_3 (and M_5 in the icosahedral case) respectively. Taking $M = \max(M_2, M_3, 2M_0)$ (or $\max(M_2, M_3, M_5, 2M_0)$ in the icosahedral case) we obtain the corollary. □

The arguments above extend some of the arguments used in the proof of [Ser77, Theorem 7] for prime levels. In fact, it is proved in [Ser77] that the nebentypus ϵ of an octahedral form of prime level must satisfy $\epsilon^4 = 1$ (this is slightly stronger than what we have obtained above, as it uses the fact that only one prime divides the level so that $\epsilon = \epsilon_p$ is an odd character!). It follows that if χ is a Dirichlet character which preserves the level of this form after twisting, then $\chi^8 = 1$. It is also shown in [Ser77] that prime levels congruent to $1 \mod 8$ do not occur (cf. part (a) of Theorem 8.1 below). It follows that $\chi^4 = 1$. In fact (see Theorem 8.2 below), there are exactly two twists of prime level; this is obvious if the level is 3 mod 4, while it follows from studying the number of invariant lines in the representation $\rho_f|_{I_p}$ when the level is 5 mod 8.

6. Octahedral Case

In this section we consider only octahedral forms. We wish to count such forms of minimal level.

In fact, we will need to avoid a certain class of minimal octahedral forms. To define this class, note that each octahedral form cuts out a non-cyclic cubic field K_3 which is the fixed field of some chosen dihedral subgroup $\mathrm{Dih}_4 \subset S_4$; we may take this Dih_4 to be

$$\{(1),(14),(23),(14)(23),(12)(34),(13)(24),(1243),(1342)\}.$$

Let K_6 be the fixed field of the group $\{(1),(14),(23),(14)(23)\}$. By Table 2 in Section 4, if $p \geq 5$ is totally ramified in K_3 (that is, has ramification type 1^3 in K_3, or equivalently $1^3 1$ in K_4), then the projective image of D_p is either

a dihedral group of order 6, or, a cyclic group of order 3.

Definition 6.1. Say a minimal octahedral newform is *good* if whenever a prime $p \geq 5$ is totally ramified in K_3, the corresponding projective image of D_p is a dihedral group of order 6 (and not a cyclic group or order 3).

An octahedral newform of prime level is both minimal and good in the above sense (cf. Section 8 below); by definition, such a form also has good level, in the sense of the introduction. In fact, any octahedral newform of good level is a good minimal form by Table 2 in Section 4, though there are presumably many more good minimal newforms than those of good level. The aim of this section is to prove the following stronger version of Theorem 1.3:

Theorem 6.2. *Let*

$$M_{\mathrm{oct}}(X) = \bigl|\{\text{good minimal octahedral cuspidal newforms } f \text{ with level } < X\}\bigr|.$$

Then $M_{\mathrm{oct}}(X) = O(X^{1+\epsilon})$.

Before we begin the proof we remark that we often consider only the prime-to-6 parts of many of the quantities involved in the argument. This is because including complete information at 2 and 3 would only change the implied constant in the result above.

Proof. To estimate $M_{\text{oct}}(X)$, we first decompose the set we wish to count according to the fields K_3:

$$M_{\text{oct}}(X) = \sum_{K_3} M_{\text{oct}}(X, K_3)$$

where $M_{\text{oct}}(X, K_3) = \big|\{f \in M_{\text{oct}}(X) \mid f \text{ cuts out } K_3\}\big|$. We now estimate $M_{\text{oct}}(X, K_3)$. Since, by Corollary 5.2, not more than $M^{\omega(\text{Level}(f))}$ different minimal forms give the same projective representation as f, we obtain:

$$M_{\text{oct}}(X, K_3) \quad = \sum_{\substack{f \text{ cuts out } K_3 \\ \text{Level}(f)<X}} 1 \quad \leq \sum_{\substack{\tilde{\rho}_f \text{ cuts out } K_3 \\ \text{Level}(f)<X}} M^{\omega(\text{Level}(f))}.$$

The projective representation $\tilde{\rho}_f$ determines and is determined by the quadratic extension K_6/K_3 (since the Galois closure of K_6/K_3 is an S_4-extension). We obtain

$$M_{\text{oct}}(X, K_3) \quad \leq \sum_{\substack{K_6/K_3 \\ \text{Level}(f)<X}} M^{\omega(\text{Level}(f))}.$$

It is a fact due to Baily [Bai80] that an arbitrary quadratic extension K_6/K_3 has Galois closure an S_4-extension if and only if $K_3/\mathbb{Q}$ has Galois closure an S_3-extension and $\text{Norm}_{\mathbb{Q}}^{K_3}(\text{Disc}(K_6/K_3)) = n^2$ is the square of some positive square-free integer n. Let n be determined by our particular quadratic extension K_6/K_3. To proceed further we need the following lemma.

Lemma 6.3. *Let f be a good minimal octahedral newform, and let* $\text{Disc}(K_3)$ *denote the discriminant of K_3. Then* $\text{lcm}(\text{Disc}(K_3), n)$ *divides* $\text{Level}(f)$ (*recall our convention of treating only the prime-to-6 parts*).

Proof. Let K_4 be a quartic field cut out by f. The following facts are easily checked:

- $p = 1^4$ in $K_4 \iff p = 1^2 1$ in K_3 and K_6/K_3 ramifies
- $p = 1^2 1^2$ or 2^2 in $K_4 \iff p$ is unramified in K_3 and K_6/K_3 ramifies
- All other ramification types for p in $K_4 \iff K_6/K_3$ is unramified.

Let $\text{Disc}(K_4)$ denote the discriminant of K_4. Then it turns out that $\text{Disc}(K_4) = \text{Disc}(K_3) \cdot n^2$. The following table (compare with Table 2 in Section 4) lists, for each $p\,(\geq 5)$, the exact power of p dividing the quantities in the statement of the lemma, in various cases:

Ram in K_4	Level(f)	Disc(K_3)	n	lcm(Disc$(K_3), n)$
1^4	p or p^2	p	p	p
$1^2 1^2$ or 2^2	p or p^2	1	p	p
Others except $1^3 1$	p or p^2	p	1	p
$1^3 1$	p^2	p^2	1	p^2

The lemma follows, since it holds in each case. □

Remark 6.4. The only case not covered by the table is the one in which p has ramification type $1^3 1$ in K_4, $p||\mathrm{Level}(f)$, $p^2||\mathrm{Disc}(K_3)$, $n = 1$, and so $p^2||\mathrm{lcm}(\mathrm{Disc}(K_3), n))$ and the lemma fails for such p. This occurs precisely when the image of D_p is $\mathbb{Z}/3\mathbb{Z}$ (instead of S_3), and explains why we have restricted to good forms.

Lemma 6.3 allows us to count octahedral forms by counting number fields. Noting that $\mathrm{Level}(f)$ and $\mathrm{lcm}(\mathrm{Disc}(K_3), n)$ have the same primes in their support (except possibly for primes dividing 6), we have:

$$\begin{aligned}
M_{\mathrm{oct}}(X, K_3) &\leq \sum_{\substack{K_6/K_3 \\ \mathrm{Level}(f)<X}} M^{\omega(\mathrm{Level}(f))} \\
&\leq \sum_{\substack{K_6/K_3 \\ \mathrm{lcm}(\mathrm{Disc}(K_3),n)<X}} M^{\omega(\mathrm{lcm}(\mathrm{Disc}(K_3),n))} \qquad \text{by Lemma 6.3} \\
&= \sum_{\substack{n \text{ square-free} \\ \mathrm{lcm}(\mathrm{Disc}(K_3),n)<X}} (\text{no. of } K_6 \leftrightarrow n) \cdot M^{\omega(\mathrm{lcm}(\mathrm{Disc}(K_3),n))}.
\end{aligned}$$

Write $n = n'n''$ where $n'' = \gcd(\mathrm{Disc}(K_3), n)$ and let $h_2^*(K_3)$ denote the 2-part of the class group of K_3. Then the number of K_6 corresponding to n is bounded above by $h_2^*(K_3) \cdot 2^{\omega(\mathrm{Disc}(K_3))} \cdot 3^{\omega(n')}$. Also $M^{\omega(\mathrm{lcm}(\mathrm{Disc}(K_3),n))} = M^{\omega(\mathrm{Disc}(K_3))} \cdot M^{\omega(n')}$. So

$$M_{\mathrm{oct}}(X, K_3) \leq h_2^*(K_3) \cdot (2M)^{\omega(\mathrm{Disc}(K_3))} \cdot \sum_{\substack{n' \text{ square-free} \\ n'<X/|\mathrm{Disc}(K_3)|}} (3M)^{\omega(n')}.$$

To proceed further we need the following lemma.

Lemma 6.5. *Let $m \geq 1$ be a fixed positive integer and let $\omega(n)$ denote the number of distinct prime divisors of n. Then*

$$\sum_{\substack{n \leq X \\ n \text{ square-free}}} m^{\omega(n)} = O(X \log^{m-1} X).$$

Proof. This follows easily by applying Perron's formula to the Dirichlet series:

$$A(s) = \sum_{\substack{n=1 \\ n \text{ square-free}}}^{\infty} \frac{m^{\omega(n)}}{n^s} = \prod_p \left(1 + \frac{m}{p^s}\right) = \zeta(s)^m G(s),$$

where $G(s)$ is a Dirichlet series with a degree $m+1$ Euler product and is holomorphic at $s = 1$. □

Applying Lemma 6.5 with $m = 3M$ to our estimate for $M_{\rm oct}(X, K_3)$ we obtain:

$$M_{\rm oct}(X, K_3) \quad \leq \quad h_2^*(K_3) \cdot (2M)^{\omega({\rm Disc}(K_3))} \cdot c \cdot \frac{X}{|{\rm Disc}(K_3)|} \log^{m-1} X$$

for some constant c. Since both $\log^{m-1}(X) = O(X^{\epsilon/4})$ and $(2M)^{\omega(d)} = O(d^{\epsilon/4})$, for any integer d, we see that:

$$M_{\rm oct}(X, K_3) \quad \leq \quad h_2^*(K_3) \cdot c \cdot X^{\epsilon/2} \cdot \frac{X}{|{\rm Disc}(K_3)|}$$

for some (new) constant c. We now wish to sum over K_3. We need one more lemma.

Lemma 6.6. *We have:*

$$\sum_{\substack{K_3 \\ |{\rm Disc}(K_3)|<X}} \frac{h_2^*(K_3)}{|{\rm Disc}(K_3)|} = O(\log X).$$

Proof. First write

$$\sum_{\substack{K_3 \\ |{\rm Disc}(K_3)|<X}} \frac{h_2^*(K_3)}{|{\rm Disc}(K_3)|} \quad = \quad \sum_{\substack{K_3 \\ |{\rm Disc}(K_3)|<X}} \frac{h_2^*(K_3)-1}{|{\rm Disc}(K_3)|} \quad + \quad \sum_{\substack{K_3 \\ |{\rm Disc}(K_3)|<X}} \frac{1}{|{\rm Disc}(K_3)|}. \tag{6.7}$$

We first show that the first sum on the right in (6.7) is $O(\log X)$. Since each K_3 gives rise to $h_2^*(K_3) - 1$ quartic fields K_4 having cubic resolvent field K_3 with ${\rm Disc}(K_4) = {\rm Disc}(K_3)$, it suffices to prove that

$$\sum_{\substack{K_4 \\ |{\rm Disc}(K_4)|<X}} \frac{1}{|{\rm Disc}(K_4)|} = O(\log X). \tag{6.8}$$

Consider the Dirichlet series

$$\sum_{K_4} \frac{1}{|{\rm Disc}(K_4)|^s}.$$

By the main result of [Bha05] (the asymptotic enumeration of quartic fields by discriminant) one has

$$\sum_{\substack{K_4 \\ |{\rm Disc}(K_4)|<X}} 1 \sim C_4 \cdot X + O(X^{1-\delta})$$

for some constant C_4 and some $\delta > 0$. For the error term see forthcoming work of Belabas-Bhargava-Pomerance [BBP, Theorem 1.3]. It now follows in a standard way that the Dirichlet series above has a simple pole at $s = 1$ (see for instance [Lang, p. 158, Theorem 4]). An application of Perron's formula shows that (6.8) holds.

To deal with the second sum in the right hand side of (6.7) we note that by the well known theorem of Davenport-Heilbronn and [BBP, Theorem 1.1] for the error term, we have

$$\sum_{\substack{K_3\\ |\mathrm{Disc}(K_3)|<X}} 1 \sim C_3 \cdot X + O(X^{1-\delta'})$$

for some constant C_3 and some $\delta' > 0$. A similar argument then shows that the second sum is also $O(\log X)$. □

Let us now sum over K_3. Using the lemma above, we obtain:

$$\begin{aligned} M_{\mathrm{oct}}(X) &= \sum_{K_3} M_{\mathrm{oct}}(X, K_3) \leq \sum_{\substack{K_3\\ |\mathrm{Disc}(K_3)|<X}} \frac{h_2^*(K_3)}{|\mathrm{Disc}(K_3)|} \cdot c \cdot X^{\epsilon/2}. = O(X^{1+\epsilon/2}\log X) \\ &= O(X^{1+\epsilon}), \end{aligned}$$

for every $\epsilon > 0$. This proves Theorem 6.2, and Theorem 1.3 also then immediately follows as a corollary. □

7. Prime sieve

In this section, we prove a bound for the number of quartic fields of bounded prime absolute discriminant. It turns out that a quartic field with prime absolute discriminant must be an S_4-*quartic field*, i.e., a quartic number field whose Galois closure has automorphism group S_4.

Indeed, if the Galois group of the Galois closure of a quartic field K_4 is V_4, $\mathbb{Z}/4$, or Dih_4, then K_4 must contain a quadratic subfield K_2, and so $\mathrm{Disc}(K_2)^2$ divides $\mathrm{Disc}(K_4)$. Meanwhile, if the Galois group of the Galois closure of K_4 is A_4, then $\mathrm{Disc}(K_4)$ must be a square. Thus $\mathrm{Disc}(K_4)$ can be prime only if it is an S_4-quartic field. Therefore, to obtain a bound on the number of quartic fields having bounded prime absolute discriminant, it suffices to restrict our attention to S_4-quartic fields.

We accomplish this by using a parametrization of S_4-*quartic orders*, i.e., orders in S_4-quartic fields. To state the result, let $V_{\mathbb{Z}}$ denote the space of pairs (A, B) of integer-coefficient ternary quadratic forms. Then, excluding degenerate cases, any element of $V_{\mathbb{Z}}$ yields two conics in $\mathbb{P}^2(\bar{\mathbb{Q}})$ which intersect in four distinct points. We say that an element $(A, B) \in V_{\mathbb{Z}}$ is *totally irreducible* if the field of definition of one (equivalently, any) of these intersection points is an S_4-quartic field. We say that two elements of $V_{\mathbb{Z}}$ are in the same *class* if one can be transformed into the other via an element of $G_{\mathbb{Z}} = \mathrm{GL}(2, \mathbb{Z}) \times \mathrm{SL}(3, \mathbb{Z})$. Finally, one finds that the action of $G_{\mathbb{Z}}$ on $V_{\mathbb{Z}}$ has a unique polynomial invariant, called the *discriminant*; it is defined by $\mathrm{Disc}(A, B) = \mathrm{Disc}(\det(Ax - By))$.

Recall that the *content* of an order R is the maximal integer n such that $R = \mathbb{Z} + nR'$ for some order R'. We then have the following theorem parametrizing S_4-quartic orders.

Theorem 7.1 ([Bha04])**.** *There is a canonical map from the set of classes of totally irreducible pairs of integer-coefficient ternary quadratic forms* (A, B) *to the set of isomorphism classes of* S_4*-quartic orders. This map preserves discriminant. Moreover, the number of pre-images of a given* (*isomorphism class of*) S_4*-quartic order* Q *is given by* $\sigma(n)$*, where* n *denotes the content of* Q *and* σ *is the usual sum-of-divisors function.*

In particular, if the absolute value of the discriminant of an S_4-quartic order is prime, then it is automatically maximal and of content 1, and will thus correspond to a unique $G_{\mathbb{Z}}$-class $(A, B) \in V_{\mathbb{Z}}$. Note that the quotient field of such an order is then an S_4-quartic field of the same prime absolute discriminant. In this section, we count S_4-quartic fields of prime absolute discriminant by counting the corresponding maximal orders, which then each correspond to a unique class in $V_{\mathbb{Z}}$.

We recall that an element $(g_2, g_3) \in \mathrm{GL}(2, \mathbb{R}) \times \mathrm{GL}(3, \mathbb{R})$ acts on the vector space $V = V_{\mathbb{Z}} \otimes \mathbb{R}$ of pairs (A, B) of ternary quadratic forms over $\mathbb{R}$ via

$$(g_2, g_3) \cdot (A, B) = (g_3 A g_3^t, g_3 B g_3^t) \cdot g_2^t.$$

The action of $G = \mathrm{GL}(2, \mathbb{R}) \times \mathrm{GL}(3, \mathbb{R})$ on V has three orbits of nonzero discriminant, namely, $V^{(0)}$, $V^{(1)}$, and $V^{(2)}$, where $V^{(i)}$ consists of those elements of V that yield a pair of conics in $\mathbb{P}^2(\mathbb{C})$ intersecting in $4-2i$ real points and $2i$ complex points. If $v \in V_{\mathbb{Z}}^{(i)} = V_{\mathbb{Z}} \cap V^{(i)}$, then the fraction field of the quartic order corresponding to v via Theorem 7.1 will then have $4 - 2i$ real embeddings and $2i$ complex embeddings.

In order to count classes of $(A, B) \in V_{\mathbb{Z}}$, we count $(A, B) \in V_{\mathbb{Z}}$ lying in certain fundamental domains for the action of $G_{\mathbb{Z}}$ on V. We construct such fundamental domains as in [Bha05, §2.1]. Namely, first let $\mathcal{F}$ be any fixed fundamental domain in $G_{\mathbb{R}} = \mathrm{GL}(2, \mathbb{R}) \times \mathrm{SL}(3, \mathbb{R})$ for $G_{\mathbb{Z}} \backslash G_{\mathbb{R}}$ that lies in a Siegel set. Then for any vector $v \in V^{(i)}$, it is clear that the multiset $\mathcal{F}v \subset V$ is the union of n_i fundamental domains for the action of $G_{\mathbb{Z}}$ on $V^{(i)}$; here $n_0 = |\mathrm{Stab}_{G_{\mathbb{R}}}(v)| = 24$ for $v \in V^{(0)}$, $n_1 = |\mathrm{Stab}_{G_{\mathbb{R}}}(v)| = 4$ for $v \in V^{(1)}$, and $n_2 = |\mathrm{Stab}_{G_{\mathbb{R}}}(v)| = 8$ for $v \in V^{(2)}$.

Note that V is a 12-dimensional real vector space. Let $H = \{w = (a_1, a_2, \ldots, a_{12}) \in V : a_1^2 + a_2^2 + \cdots + a_{12}^2 \leq 10, \ |\mathrm{Disc}(w)| \geq 1\}$. Given a subset S of $V_{\mathbb{Z}}$, by "the expected number of elements of S in a fundamental domain for $G_{\mathbb{Z}} \backslash V^{(i)}$", we mean the expected number of points of S lying in $\mathcal{F}v$ divided by n_i, as v ranges over $H \cap V^{(i)}$ with respect to the measure $|\mathrm{Disc}(v)|^{-1} dv$. (For more details on the reasons for this choice of set H and measure $|\mathrm{Disc}(v)|^{-1} dv$, see [Bha05].)

Now to count the number of totally irreducible classes of $(A,B)\in V_{\mathbb{Z}}$ having prime absolute discriminant, we first count all classes of $(A,B)\in V_{\mathbb{Z}}$ having discriminant a multiple of any given square-free number q. To state this result, we require some terminology and some auxiliary lemmas. First, for a pair of ternary quadratic forms $(A,B)\in V$, where $A(x_1,x_2,x_3)=\sum_{i\le j}a_{ij}x_ix_j$ and $B(x_1,x_2,x_3)=\sum_{i\le j}b_{ij}x_ix_j$, we say that the *first coordinate of* (A,B) is a_{11}, while the *first four coordinates of* (A,B) are given by a_{11}, a_{12}, a_{13}, and a_{22}.

The following lemma ([Bha05, Lemma 11]) indicates how often the first coordinate a_{11} vanishes in a fundamental domain for $G_{\mathbb{Z}}\backslash V_{\mathbb{Z}}$:

Lemma 7.2. *The expected number of $(A,B)\in\mathcal{F}v$ $(v\in H)$ with $a_{11}=0$ that are totally irreducible and have absolute discriminant less than X is $O(X^{11/12})$.*

The next lemma similarly bounds the expected number of points in a fundamental domain $\mathcal{F}v$ $(v\in H)$ that are not totally irreducible but for which the first coordinate a_{11} is nonzero:

Lemma 7.3. *The number of $(A,B)\in\mathcal{F}v$ $(v\in H)$ with $a_{11}\neq 0$ that are not totally irreducible and have absolute discriminant less than X is $O(X^{11/12+\epsilon})$.*

Proof. This follows from [Bha05, Lemmas 12 and 13] and [Won99]. □

Thus, up to an error of $O(X^{11/12+\epsilon})$, we see that to count the expected number of totally irreducible elements in $\mathcal{F}v$ $(v\in H)$ having bounded discriminant, it suffices to count all elements in $\mathcal{F}v$ having nonzero first coordinate. To this end, we may state the following counting result (see [BBP, Theorem 4.10]):

Theorem 7.4. *For a positive integer m, let L be any translate $v+m\cdot V_{\mathbb{Z}}$ $(v\in V_{\mathbb{Z}})$ of the sublattice $m\cdot V_{\mathbb{Z}}$ of $V_{\mathbb{Z}}$, and let (a,b,c,d) denote the smallest positive first four coordinates of any element in L. For $i=0,1,2$, let $N^{(i)}(L;X)$ denote the expected number of lattice points in L, with first coordinate nonzero and discriminant less than X, lying in a fundamental domain for $G_{\mathbb{Z}}\backslash V^{(i)}$. Then*

$$\begin{aligned} N^{(i)}(L;X) &= m^{-12}\,N^{(i)}(1,X)\\ &\quad + O\Big(\sum_{S\subset\{a_{ij},b_{ij}\}} m^{-|S|}a^{-\alpha_S}b^{-\beta_S}c^{-\gamma_S}d^{-\delta_S}X^{(|S|+\alpha_S+\beta_S+\gamma_S+\delta_S)/12}+\log X\Big), \end{aligned} \tag{7.5}$$

where S ranges over the nonempty proper subsets of the set of 12 coordinates $\{a_{ij},b_{ij}\}$ on $V_{\mathbb{Z}}$, and $\alpha_S,\beta_S,\gamma_S,\delta_S\in[0,1]$ are real constants that depend only on S and satisfy $|S|+\alpha_S+\beta_S+\gamma_S+\delta_S\le 11$. Moreover, it is possible to choose $\alpha_S,\beta_S,\gamma_S,\delta_S\in[0,1)$ for all S except for the following three sets:

(1) $\{b_{11}, b_{12}, b_{13}, b_{22}, b_{23}, b_{33}\}$, *for which* α_S, β_S, γ_S, $\delta_S = 1$*;*
(2) $\{a_{13}, a_{23}, a_{33}, b_{13}, b_{23}, b_{33}\}$, *for which* $\gamma_S = 0$ *and* α_S, β_S, $\delta_S = 1$*;*
(3) $\{a_{22}, a_{23}, a_{33}, b_{22}, b_{23}, b_{33}\}$, *for which* $\delta_S = 0$ *and* α_S, β_S, $\gamma_S = 1$.

Let $Z(q)$ denote the set of all elements in $V_{\mathbb{Z}}$ whose discriminant is a multiple of q. Since the discriminant is an integer polynomial on the coordinates of $V_{\mathbb{Z}}$, the set $Z(q)$ may be expressed as the union of some number k of translates $L_1, \ldots, L_k$ of the lattice $q \cdot V_{\mathbb{Z}}$. The following result gives us the number k as a function of q.

Lemma 7.6. *Let $g(q)$ be the multiplicative function defined on square-free numbers q, where for a prime p,*

$$g(p) \quad = \quad (p^{11} + 2p^{10} - p^9 - 2p^8 - p^7 + 2p^6 + p^5 - p^4)/p^{12}.$$

Then the number k of translates of the lattice $q \cdot V_{\mathbb{Z}}$ that comprise $Z(q)$ is $g(q)q^{12}$.

Proof. By the Chinese Remainder Theorem, it suffices to consider the case where $q = p$ is a prime. With notation as in [Bha04], we have that an element $(A, B) \in V_{\mathbb{Z}}$ has discriminant coprime to p if and only if $(A, B) \in T_p(1111)$, $T_p(112)$, $T_p(13)$, $T_p(4)$, or $T_p(22)$. Lemma 23 in [Bha04] gives the number of translates of $p \cdot V_{\mathbb{Z}}$ lying in each of these five sets. Subtracting the total number of these translates from p^{12} yields

$$p^{12} - p^4(p-1)^4(p+1)^2(p^2+p+1),$$

implying the lemma. □

Now in each translate L of $q \cdot V_{\mathbb{Z}}$, we consider its *standard member* as the one with each entry in the interval $[1, q]$. (Indeed, the space of pairs of ternary quadratic forms $V_{\mathbb{Z}}$ may be thought of as the lattice $\mathbb{Z}^{12}$, and so L, as a coset of $q \cdot V_{\mathbb{Z}}$, has each of its twelve entries running independently over particular residue classes modulo q.) For each of the k translates $L_1, \ldots, L_k$ of $q \cdot V_{\mathbb{Z}}$ which comprise $Z(q)$, let $(a_1, b_1, c_1, d_1), \ldots, (a_k, b_k, c_k, d_k)$ denote the respective quadruples consisting of the first four coordinates of their standard members. Thus, $(a_1, b_1, c_1, d_1), \ldots, (a_k, b_k, c_k, d_k)$ are all quadruples of integers in $[1, q]^4 = [1, q] \times [1, q] \times [1, q] \times [1, q]$, and from Lemma 7.6, there are $k = g(q)q^{12}$ of them.

We now describe the distribution of these k quadruples. We begin with the following lemma.

Lemma 7.7. *Suppose A is a ternary quadratic form over $\mathbb{Z}$, and let p be any prime. Let* $\mathrm{rk}(A)$ *denote the rank of A over $\mathbb{Z}/p\mathbb{Z}$. Then the number of values* $\pmod p$ *for the quadratic* *form B, such that* $\mathrm{Disc}(A,B)\equiv 0 \pmod p$*, is*

$$\begin{array}{rll} p^5 & +\,O(p^4), & \textit{if}\ \mathrm{rk}(A)=3;\\ \le 3p^5 & +\,O(p^4), & \textit{if}\ \mathrm{rk}(A)=2;\\ p^6, & & \textit{if}\ \mathrm{rk}(A)\le 1. \end{array}$$

Proof. Suppose $\mathrm{rk}(A)=3$. We view A and B as conics in $\mathbb{P}^2(\bar{\mathbb{F}}_p)$. For $\mathrm{Disc}(A,B)\equiv 0 \pmod p$ to hold, A and B must have a multiple point of intersection in $\mathbb{P}^2(\bar{\mathbb{F}}_p)$. The number of $B \pmod p$ with this property is $p^5+O(p^4)$. Indeed, A has $p+1$ points in $\mathbb{P}^2(\mathbb{F}_p)$, and the number of B that have at least a double intersection at a given $\mathbb{F}_p$-rational point of A is $p^4+O(p^3)$ (as this amounts to two linear conditions on B mod p). Thus the total number of B having a multiple point of intersection at an $\mathbb{F}_p$-rational point of A is $p^5+O(p^4)$. Finally, it is easy to see that the number of B having more than one multiple point of intersection with A in $\mathbb{P}^2(\bar{\mathbb{F}}_p)$ is negligible in comparison, i.e., $O(p^4)$, yielding the desired result in this case.

If $\mathrm{rk}(A)=2$, then in $\mathbb{P}^2(\bar{\mathbb{F}}_p)$, the degenerate conic A is the union of two distinct lines. The number of $B \pmod p$ having a multiple intersection point with A is then at most $2p^5+p^5+O(p^4)=3p^5+O(p^4)$, giving the lemma in this case.

If $\mathrm{rk}(A)=1$, then in $\mathbb{P}^2(\mathbb{F}_p)$, the (degenerate) conic A is a double line. Any B will have a multiple intersection with A, when viewed as conics in $\mathbb{P}^2(\mathbb{F}_p)$. Thus we obtain p^6 values of B in this case. Lastly, if $\mathrm{rk}(A)=0$, then again B can be any ternary quadratic form, as all p^6 values of B will give an (A,B) whose discriminant is a multiple of p. This completes the proof. □

We now prove the following proposition which gives information on the distribution of the quadruple $(a_{11},a_{12},a_{13},a_{22})=(a,b,c,d)$ in $Z(p)$.

Proposition 7.8. *Fix* $a,b,c,d\in\mathbb{Z}/p\mathbb{Z}$*. Then modulo* p*, the number of* $(A,B)\in Z(p)$ *with given values of* a,b,c,d *is*

$$\begin{array}{rll} p^7 & +\,O(p^6), & \textit{if}\ b^2-4ad\not\equiv 0 \pmod p;\\ \le 3p^7 & +\,O(p^6), & \textit{if}\ b^2-4ad\equiv 0 \pmod p\ \textit{but}\ \gcd(a,c)\not\equiv 0 \pmod p);\\ \le 2p^7 & +\,O(p^6), & \textit{otherwise}. \end{array}$$

Proof. If $b^2-4ad\not\equiv 0 \pmod p$, then $\mathrm{Det}(A)$, as a polynomial function of $u=a_{23}$ and $v=a_{33}$, does not identically vanish $\pmod p$. Hence the number of possible values of u, $v \pmod p$ for which $\mathrm{Det}(A)$ is nonzero $\pmod p$ is $p^2+O(p)$. By Lemma 7.7, the number of values of (A,B) with $\mathrm{rk}(A)=3$, $\mathrm{Disc}(A,B)\equiv 0 \pmod p$, and the given values of a,b,c,d, is $(p^2+O(p))(p^5+O(p^4))=p^7+O(p^6)$.

We now consider those $O(p)$ choices of $u, v \pmod p$ for which A has vanishing determinant $\pmod p$. The rank of $A \pmod p$ will then be 2. By Lemma 7.7, the number of values of $(A, B) \pmod p$ with $\mathrm{rk}(A) = 2$, $(A, B) \in Z(p)$, and the given values of a, b, c, d, is at most $(O(p))(3p^5 + O(p^4)) = O(p^6)$. This takes care of the first case.

Suppose we are now in the second case, i.e., $b^2 - 4ad \equiv 0 \pmod p$ but at least one of $a, c \not\equiv 0 \pmod p$. In this case, by the same argument as in the first case, we have at most $3p^7 + O(p^6)$ possible values for $(A, B) \pmod p$ with $\mathrm{rk}(A) \geq 2$, $(A, B) \in Z(p)$, and the given values of a, b, c, d. However, in this second case, we also have the possibility $\mathrm{rk}(A) = 1$. Note that $A \pmod p$ will be of rank 1 only if $c^2 - 4av \equiv bc - 2au \equiv 0$. If a is nonzero $\pmod p$, then (assuming $p > 2$) v and u are determined $\pmod p$ by the given information, so there are is at most one choice possible for the pair $(u, v) \pmod p$ for which the condition $\mathrm{rk}(A) = 1$ holds. If a is zero $\pmod p$, then for $\mathrm{rk}(A) = 1$ to hold, we also then need $c \equiv 0 \pmod p$, a contradiction. Thus, regardless of the value of a, there is at most one value of $u, v \pmod p$ yielding $\mathrm{rk}(A) = 1$. By Lemma 7.7, we conclude that the number of values of (A, B) with $\mathrm{rk}(A) = 1$, $(A, B) \in Z(p)$, and our given values of a, b, c, d is at most $1(p^6 + O(p^5))$, which takes care of this case.

Finally, we consider the last case where $b^2 - 4ad \equiv a \equiv c \equiv 0 \pmod p$, which also implies $b \equiv 0 \pmod p$. The condition on a, b, c, d implies that $\mathrm{Det}(A)$ vanishes $\pmod p$. Thus the rank of A is at most 2, regardless of u and v. The number of values of u and $v \pmod p$ with $\mathrm{rk}(A) = 2$ is thus less than p^2; by Lemma 7.7, the number of $(A, B) \in Z(p)$, with $\mathrm{rk}(A) = 2$ and the given values of a, b, c, d, is at most $p^7 + O(p^6)$.

For $A \pmod p$ to be rank ≤ 1 for some values of u and v, we must have $u^2 \equiv 4dv \pmod p$, so if d is not zero $\pmod p$, then $v \pmod p$ is determined by u (assuming $p > 2$), while if $d \equiv 0 \pmod p$, then $u \equiv 0 \pmod p$ and v may be any value $\pmod p$. Thus, regardless of the value of d, the number of values of u and $v \pmod p$ with $\mathrm{rk}(A) = 1$ in this case is $p + O(1)$. By Lemma 7.7, the number of (A, B) with discriminant a multiple of p, $\mathrm{rk}(A) = 1$, and the given values of a, b, c, d, is $(p + O(1))(p^6 + O(p^5)) = p^7 + O(p^6)$. This completes the proof of the proposition. □

Corollary 7.9. *Let q be square-free and let (a, b, c, d) be a quadruple of integers in $[1, q]^4$. The number of translates L_j of $q \cdot V_{\mathbb{Z}}$ that comprise $Z(q)$ and have (a, b, c, d) as the first four coordinates of some member is*

$$3^f \left(q^7 + O(q^6)\right),$$

where

$$0 \leq f \leq \sum_{p \mid \gcd(q, b^2 - 4ad)} 1.$$

For $i = 0, 1, 2$, and for any subset $S \subset V_{\mathbb{Z}}$, let $N^{(i)}_{\mathrm{irr}}(S; X)$ denote the expected number of totally irreducible lattice points in S lying in a fundamental domain for $G_{\mathbb{Z}}\backslash V^{(i)}$ having absolute discriminant less than X. The following proposition then follows from Lemma 7.2, Lemma 7.3, Theorem 7.4, Lemma 7.6, and Corollary 7.9. The proof is essentially identical to [BBP, Cor. 4.11].

Proposition 7.10. *Let q be a square-free integer. Then*

$$N^{(i)}_{\mathrm{irr}}(Z(q); X) = g(q)N^{(i)}(V_{\mathbb{Z}}, X) + O\left(\left(\frac{q}{\varphi(q)}\right)^{\theta}\left(X^{11/12} + q^{11}\log X\right) + X^{11/12+\epsilon}\right).$$

The constant θ in this result depends on the the O-constant in Corollary 7.9, the function $f(a, b, c, d)$ there, and also on the fact that $g(q)q = O\left((q/\varphi(q))^2\right)$. The exact determination of θ is unimportant to our results.

Let $N_4^{\mathrm{prime}}(X)$ denote the number of S_4-quartic fields having absolute discriminant a prime less than X. It is well-known from sieve-theory that a result of the nature of Proposition 7.10, which gives an asymptotic (with sufficiently strong error term) for the number of fields of discriminant a multiple of q for any square-free q, implies that the number $N_4^{\mathrm{prime}}(X)$ of S_4-quartic fields of prime absolute discriminant less than X is $O(X/\log X)$. We have proven:

Theorem 7.11. *There exists a constant C such that*

$$\limsup_{X\to\infty} \frac{N_4^{\mathrm{prime}}(X)}{(X/\log X)} < C.$$

In fact, naively inserting the result of Proposition 7.10 into Iwaniec's refinement of Rosser's sieve [Iwa80, Theorem 1], we find that we may take, e.g., $C = 5$ in Theorem 7.11, although this value of C could certainly be lowered with additional work. Indeed, to obtain a rough estimate for C, let $N_4^{\mathrm{prime},(i)}(X)$ be the number of quartic fields of prime discriminant (in absolute value) less than X, with $4 - 2i$ real embeddings and $2i$ complex embeddings, so that $N_4^{\mathrm{prime}}(X) = \sum_{i=0}^{2} N_4^{\mathrm{prime},(i)}(X)$. A short computation shows that

$$\prod_{p<z}(1 - g(p)) = \frac{1}{\zeta(2)^2\zeta(3)}\frac{e^{-\gamma}}{\log z}(1 + \text{error term})$$

where γ is Euler's constant. Hence, by Proposition 7.10, [Iwa80, Theorem 1] and [Bha05, Theorem 7] we see that $N_4^{\mathrm{prime},(i)}(X) < C_i X/\log X$ + error term, where C_i can be taken to be the smallest value that the expression $\frac{1}{\zeta(2)^2\zeta(3)}e^{-\gamma}(2e^{\gamma}/\alpha s)(\zeta(2)^2\zeta(3)/2n_i)$ takes subject to $\alpha s < 1/12$, that is, we may take C_i to be $12/n_i$. Thus C may be taken to be $\sum_{i=0}^{2} C_i = 5$.

Theorem 7.11 thus states that there are fewer than C quartic fields of absolute discriminant $|D|$ on average, for prime values of $|D|$. By the duality between quartic fields and 2-torsion elements in the class groups of cubic fields, we thus also obtain:

Corollary 7.12. *With C as in Theorem 7.11, we have*

$$\sum_{|\mathrm{Disc}(K_3)| \text{ prime } < X} h_2^*(K_3) < CX/\log X$$

for sufficiently large values of X.

8. Prime Conductor

Finally, let us count forms of prime conductor. Such forms are necessarily minimal (that is have minimal level amongst their twists). Moreover octahedral forms of prime level are good in the sense of definition 6.1, as follows from the following results of Tate written down by Serre [Ser77].

Theorem 8.1 ([Ser77, Thm. 7]). *Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ be an irreducible odd representation of prime conductor p. Assume that ρ is not dihedral.*

(a) *Then $p \not\equiv 1 \mod 8$*
(b) *If $p \equiv 5 \mod 8$, then ρ is of octahedral type*
(c) *If $p \equiv 3 \mod 4$, then ρ is of octahedral type or of icosahedral type.*

Conversely, suppose we start with a Galois extension $E/\mathbb{Q}$ and a prime p. Consider the three cases:

(b) $\mathrm{Gal}(E/\mathbb{Q}) \cong S_4$ and $p \equiv 5 \mod 8$
(c1) $\mathrm{Gal}(E/\mathbb{Q}) \cong S_4$ and $p \equiv 3 \mod 4$
(c2) $\mathrm{Gal}(E/\mathbb{Q}) \cong A_5$ and $p \equiv 3 \mod 4$.

Fix an embedding of $\mathrm{Gal}(E/\mathbb{Q})$ in $\mathrm{PGL}_2(\mathbb{C})$. In the octahedral case (respectively, icosahedral case) there is only one (respectively, two) such embedding(s) up to conjugacy. Let $\tilde{\rho}_E$ denote the induced projective representation of $G_{\mathbb{Q}}$.

Theorem 8.2 ([Ser77, Thm. 8]). *$\tilde{\rho}_E$ has a lift with conductor p and odd determinant if and only if E is the normal closure of a non-real*

(b) *quartic field $K/\mathbb{Q}$ with discriminant p^3*
(c1) *quartic field $K/\mathbb{Q}$ with discriminant $-p$*
(c2) *quintic field $K/\mathbb{Q}$ with discriminant p^2.*

When these conditions are satisfied, in each case $\tilde{\rho}_E$ has precisely two non-isomorphic liftings with odd determinant and conductor p.

We now prove Theorem 1.2, i.e., that $N_{\text{oct}}^{\text{prime}}(X) = O(X/\log X)$.

Proof. As usual let K_3 denote the fixed field of the dihedral group $\text{Dih}_4 \subset S_4$ fixed in Section 6 and let K_6/K_3 be the corresponding quadratic extension. Recall $\text{Norm}_{\mathbb{Q}}^{K_3}(\text{Disc}(K_6/K_3)) = n^2$. By Theorem 8.2, we see that there are only two possibilities for the ramification of p. These are summarized in the following table:

Ram in K_4	Level(f)	Ram in K_3	$\lvert\text{Disc}(K_3)\rvert$	n
1^4	p	11^2	p	p
111^2	p	11^2	p	1

Moreover, the first possibility can occur only when K_4 is totally complex, and the second only when K_4 is of mixed signature.

Let $N_{\text{oct}}^{\text{prime}}(X, K_3) = \big|\{f \text{ such that Level}(f) \text{ is a prime } < X \text{ and } f \text{ cuts out } K_3\}\big|$. Then $N_{\text{oct}}^{\text{prime}}(X) = \sum_{K_3} N_{\text{oct}}^{\text{prime}}(X, K_3)$. Since each S_4 extension gives rise to two f's (by Theorem 8.2 above), we have:

$$\begin{aligned}
N_{\text{oct}}^{\text{prime}}(X, K_3) &= \sum_{\substack{K_6/K_3 \\ \text{Level}(f)<X}} 2 \\
&= \sum_{\substack{K_6/K_3 \\ \text{lcm}(\text{Disc}(K_3),n)<X}} 2 \\
&= 2 \sum_{\substack{K_6/K_3 \\ \text{lcm}(\text{Disc}(K_3),n)<X}} (\text{no. of } K_6 \leftrightarrow n) \\
&\leq 4\, h_2^*(K_3),
\end{aligned}$$

since in the last sum n is uniquely determined to be $\text{Disc}(K_3)$ or 1 in accordance with whether K_3 is totally real or of mixed signature. Note that the number of K_6's corresponding to n when $n = \text{Disc}(K_3)$ (i.e., when K_3 is totally real) is $2^{\omega(\text{Disc}(K_3))} h_2^*(K_3) = 2h_2^*(K_3)$, and is $h_2^*(K_3)$ otherwise.

Hence

$$N_{\text{oct}}^{\text{prime}}(X) = \sum_{|\text{Disc}(K_3)| \text{ prime } < X} N_{\text{oct}}^{\text{prime}}(X, K_3) \leq \sum_{|\text{Disc}(K_3)| \text{ prime } < X} 4h_2^*(K_3) < 4CX/\log X$$

for sufficiently large X, by Corollary 7.12. This concludes the proof. □

References

[Bai80] A. Baily. On the density of discriminants of quartic fields. *J. Reine Angew. Math.* **315** (1980), 190–210.

[BBP] K. Belabas, M. Bhargava, and C. Pomerance. Error estimates for the Davenport-Heilbronn theorems. *Preprint* (2008).

[Bha04] M. Bhargava. Higher composition laws III: The parametrization of quartic rings. *Ann. of Math.* **159** (2004), no. 3, 1329–1360.

[Bha05] M. Bhargava. The density of discriminants of quartic rings and fields. *Ann. of Math.* **162** (2005), no. 2, 1031–1063.

[Duk95] W. Duke. The dimension of the space of cusp forms of weight one. *Internat. Math. Res. Notices* **1995**, no. 2, 99–109.

[Ell03] J. Ellenberg. On the average number of octahedral modular forms. *Math. Res. Lett.* **10** (2003), no. 2-3, 269–273.

[Fre94] G. Frey (Editor). On Artin's conjecture for odd 2-dimensional representations. *Lecture Notes in Mathematics* **1585**, Springer-Verlag, Berlin, 1994.

[Gan06] S. Ganguly. Large sieve inequalities and application to counting modular forms of weight one. *Ph. D. thesis, Rutgers University*, 2006.

[Iwa80] H. Iwaniec. Rosser's sieve. *Acta Arith.* **36** (1980), no. 2, 171–202.

[Klu06] J. Klüners. The number of S_4-fields with given discriminant. *Acta. Arith.* **122** (2006), no. 2, 185–194.

[Lang] S. Lang. *Algebraic Number Theory.* Second edition, Graduate Texts in Mathematics **110**, Springer-Verlag, New York, 1994.

[MV02] P. Michel and A. Venkatesh. On the dimension of the space of cusp forms associated to 2-dimensional complex Galois representations. *Int. Math. Res. Not.* **2002**, no. 38, 2021–2027.

[Ser77] J-P. Serre. Modular forms of weight one and Galois representations. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pp. 193–268. Academic Press, London, 1977.

[Won99] S. Wong. Automorphic forms on GL(2) and the rank of class groups. *J. Reine Angew. Math.* **515** (1999), 125–153.

Department of Mathematics, Princeton University, Princeton, NJ 08544, USA.
E-mail address: bhargava@math.princeton.edu

School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai 400005, India.
E-mail address: eghate@math.tifr.res.in