ACTA ARITHMETICA
122.2 (2006)

The number of S_4-fields with given discriminant

by

JÜRGEN KLÜNERS (Kassel)

1. Introduction. For a number field k we denote by $d_k \in \mathbb{N}$ the absolute value of the field discriminant of k. The class group will be denoted by Cl_k and the *p-rank* $\mathrm{rk}_p(A)$ of an abelian group A is defined to be the minimal number of generators of A/A^p. We denote by $\mathcal{N}$ the absolute norm. The symbol O_ε denotes the usual Landau symbol O, where the implied constant is depending on ε.

In this note we answer a question of Akshay Venkatesh about the number of S_4-extensions of degree 4 with given discriminant d. It is conjectured that this number is $O_\varepsilon(d^\varepsilon)$ for all $\varepsilon > 0$. On average we have the stronger result (see [Bha02, Bel04])

$$\lim_{x\to\infty} \frac{1}{x} \sum_{K: d_K \le x} 1 = c(S_4),$$

where K runs through all quartic S_4-extensions and $c(S_4) > 0$ is explicitly given. We prove the bound $O_\varepsilon(d^{1/2+\varepsilon})$ for all $\varepsilon > 0$, which improves the bound $O_\varepsilon(d^{4/5+\varepsilon})$ given in [MV02].

As an application we give an upper bound for the dimension of the space of octahedral forms of weight 1 and given conductor N. In the general case the best known bound is $O_\varepsilon(N^{4/5+\varepsilon})$ for all $\varepsilon > 0$, given in [MV02]. For squarefree conductors this bound is improved to $O_\varepsilon(N^{2/3+\varepsilon})$ on average. In this note we are able to prove the upper bound $O_\varepsilon(N^{1/2+\varepsilon})$ in many cases, e.g. when N is prime or a square.

The discrepancy between the expected bound $O_\varepsilon(d^\varepsilon)$ and the proven bound $O_\varepsilon(d^{1/2+\varepsilon})$ for the number of S_4-extensions of discriminant d comes from the fact that we can only use weak bounds for the 3-rank of the class group of quadratic fields and the 2-rank of the class group of non-cyclic cubic fields.

In order to understand the problems which arise we give the following easy example. Let us count the number of cubic S_3-extensions $M/\mathbb{Q}$ of

2000 *Mathematics Subject Classification*: Primary 11R29; Secondary 11R16, 11R32.

discriminant d such that the normal closure contains a given quadratic extension k. Since every unramified cyclic cubic extension N/k corresponds to a cubic extension M we see that the number of elements h_3 of order 3 in the class group Cl_k plays an important role. In the general case we can only use the estimate $h_3 \le \#\mathrm{Cl}_k$ and the latter can be bounded by $O(d^{1/2}\log(d))$ using Lemma 2 below. It is very difficult to improve this trivial bound for elements of order p in the class group when $p > 3$. Just recently for $p = 3$ Helfgott and Venkatesh [HV04] ($\lambda = 0.44179$) and independently Pierce [Pie05] ($\lambda = 0.49108$ or $\lambda = 0.41667$ in special cases) proved that for all $\varepsilon > 0$ we get

$$3^{\mathrm{rk}_3(\mathrm{Cl}_k)} = O_\varepsilon(d_k^{\lambda+\varepsilon}).$$

Using this improved bound it is straightforward to get the upper bound $O_\varepsilon(d^{\lambda+\varepsilon})$ for the number of cubic S_3-extensions.

In the following we would like to explain the idea of the proof of our main result. We will improve the following elementary approach given in [Duk95, p. 101]. In the worst case we cannot exclude the possibility that there exists a quadratic field $k/\mathbb{Q}$ such that $3^{\mathrm{rk}_3(\mathrm{Cl}_k)} = O(d_k^{1/2}\log(d_k))$. Using these unramified C_3-extensions of k there are $\frac{3^{\mathrm{rk}_3(\mathrm{Cl}_k)}-1}{3-1}$ non-cyclic cubic fields M of the same discriminant. In the worst case all these extensions have a large 2-rank, i.e.

$$2^{\mathrm{rk}_2(\mathrm{Cl}_M)} = O(d_M^{1/2}\log(d_M)^2).$$

Every unramified C_2-extension leads to an S_4-extension K of degree 4 of the same discriminant $d_K = d_k = d_M$. Using this idea we get the upper bound $O(d_K\log(d_K)^3)$ for the number of S_4-extensions of discriminant d_K.

As we see from the above example, there is a problem for our upper estimates when $\mathrm{rk}_2(\mathrm{Cl}_M)$ and $\mathrm{rk}_3(\mathrm{Cl}_k)$ are large. We will use Theorem 1 below, proved by Frank Gerth III, which says that $\mathrm{rk}_3(\mathrm{Cl}_M)$ has about the same size as $\mathrm{rk}_3(\mathrm{Cl}_k)$. This means that $\mathrm{rk}_3(\mathrm{Cl}_M)$ is large when $\mathrm{rk}_3(\mathrm{Cl}_k)$ is large. This in turn implies that $\mathrm{rk}_2(\mathrm{Cl}_M)$ must be small.

For instance, consider the special case that d is squarefree, i.e. the corresponding S_3-extension L is unramified over k. Then the first part of Theorem 1 and the above-explained elementary approach already proves our desired result, i.e. the number of S_4-extensions of discriminant d is bounded by $O(d^{1/2+\varepsilon})$.

2. Parameterizing S_4-extensions. Let $K/\mathbb{Q}$ be a quartic field such that the normal closure N has Galois group S_4. Then there is a unique normal subfield L of degree 6 with Galois group S_3. We denote by M a subfield of L of degree 3 and by k the unique subfield of degree 2 of L (or N):

$$\begin{tikzcd}
& N \arrow[d, dash, "4"'] \arrow[ddr, dash, "6"] & \\
& L \arrow[dl, dash, "2"'] \arrow[dd, dash, "3"'] & \\
M \arrow[ddr, dash, "S_3"'] & & K \arrow[ddl, dash, "S_4"] \\
& k \arrow[d, dash, "2"] & \\
& \mathbb{Q} &
\end{tikzcd}$$

For $n \in \mathbb{N}$ we define

$$\operatorname{Rad}(n) := \prod_{p \mid n} p,$$

where the product is only taken over primes. To each $K/\mathbb{Q}$ as above we associate a triple

$$(a, b, c) = (\operatorname{Rad}(d_k), \operatorname{Rad}(\mathcal{N}(d_{L/k})), \operatorname{Rad}(\mathcal{N}(d_{N/L}))) \in \mathbb{N}^3$$

of squarefree numbers. We define

$$\Psi : \mathcal{K} \to \mathbb{N}^3, \qquad K \mapsto (a, b, c), \tag{1}$$

where $\mathcal{K}$ is the set of quartic S_4-extensions of $\mathbb{Q}$ up to isomorphism. Ψ is a well defined mapping with bounded fibres. In the rest of this section we want to give upper bounds for the size of the fibres, i.e. to give an upper bound for the number of fields K which are associated to a given triple (a, b, c).

Assuming this situation k is one of the following quadratic fields. If $2 \nmid a$ we get $k = \mathbb{Q}(\sqrt{\pm a})$ where the sign is positive if $a \equiv 1 \bmod 4$. If $2 \mid a$ then k is one of the following three fields: $\mathbb{Q}(\sqrt{a}), \mathbb{Q}(\sqrt{-a})$, and $\mathbb{Q}(\sqrt{\pm a/2})$, where the sign is positive when $a/2 \equiv 3 \bmod 4$. Therefore at most 3 quadratic fields are associated to a given a. The number of b's for a given field k can be easily bounded by the following lemma; we denote by $\omega(b)$ the number of prime factors of b.

LEMMA 1. *Let $b \in \mathbb{N}$ as above. Then all fields M (up to isomorphism) such that L/K is only ramified at primes dividing b are contained in the ray class field of $\mathfrak{a} := 3b\mathcal{O}_k$. The number of those extensions can be bounded by*

$$\frac{3^r - 1}{3 - 1}, \qquad \textit{where } r = \operatorname{rk}_3(\operatorname{Cl}_k) + \omega(b) + 2.$$

Proof. We are looking for all fields which are at most ramified at primes dividing b. We need to choose $\mathfrak{a}$ in such a way that all these fields are subfields of the ray class field of $\mathfrak{a}$. For primes $\mathfrak{p}$ not dividing 3 it is sufficient that $\mathfrak{p} \mid \mathfrak{a}$. For the wildly ramified primes there exists a maximal exponent such that all these fields occur as subfields [Ser95, p. 58] of the ray class

field of $\mathfrak{a}$. Using elementary properties of the ray class group $\mathrm{Cl}_\mathfrak{a}$ we get
$$\mathrm{rk}_3(\mathrm{Cl}_\mathfrak{a}) \le \mathrm{rk}_3(\mathrm{Cl}_k) + \mathrm{rk}_3((\mathcal{O}_k/\mathfrak{a})^*).$$
For all prime ideals $\mathfrak{p}$ not dividing 3 we find that the 3-rank of $(\mathcal{O}_k/\mathfrak{p})^*$ is at most 1, which shows that $\mathrm{rk}_3(\mathcal{O}_k/p\mathcal{O}_k) \le 2$. Equality can only occur in the case $p \equiv 1 \bmod 3$, where $p \in \mathbb{P} \cap \mathfrak{p}$. In this case there exists a C_3-extension of $\mathbb{Q}$ only ramified at p. Denote by A the 3-part of the ray class group $\mathrm{Cl}_\mathfrak{a}$. We can write $A := A^+ \oplus A^-$, where the classes in A^+ are invariant under $\mathrm{Gal}(k/\mathbb{Q})$. Because a prime $p \equiv 1 \bmod 3$ increases the 3-rank of A^+ by one, we see that all odd primes increase the 3-rank of A^- by at most one. The theory used in [FK03, Section 6] shows that S_3-extensions correspond to quotients of index 3 of A^-. Finally, we need to estimate the 3-rank for $(\mathcal{O}_k/\mathfrak{p}^w)^*$ for primes dividing 3. In [HPP03] it is proved that the p-rank of $(\mathcal{O}_k/\mathfrak{p}^w)^*$ is at most $[k_\mathfrak{p} : \mathbb{Q}_p] + 1$. In all cases it is sufficient to add 2 since there is one C_3-extension of $\mathbb{Q}$ only ramified at 3. ∎

We use the trivial class group bound which can be found in [Nar90, Theorem 4.4].

LEMMA 2. *For all $n \in \mathbb{N}$ there exists a constant $c(n)$ such that for all number fields F of degree n we have*
$$|\mathrm{Cl}_F| \le c(n) d_F^{1/2} \log(d_F)^{n-1}.$$

Trivially, we have $3^{\mathrm{rk}_3(\mathrm{Cl}_k)} \le |\mathrm{Cl}_k|$. For a given cubic S_3-field M we prove a lemma similar to Lemma 1.

LEMMA 3. *Let $c \in \mathbb{N}$ be as above. Then the number of S_4-extensions N which contain a given S_3-field M such that $\mathcal{N}(d_{N/L})$ is only divisible by primes dividing c is bounded by*
$$2^r - 1, \qquad \textit{where } r = \mathrm{rk}_2(\mathrm{Cl}_M) + 3\omega(c) + 6.$$

Proof. In [Bai80, Lemmata 4, 5] it is proven that the Galois closure of $M(\sqrt{\alpha})$ for $\alpha \in M$ has Galois group S_4 if and only if $\mathcal{N}(\alpha)$ is a square. If $\mathcal{N}(\alpha)$ is a square this certainly implies that the norm of the principal ideal (α) is a square. Therefore we get an upper bound if we count all extensions such that the conductor is a square. For a prime $p \neq 3$ we have at most three possibilities to produce squarefree ideals of norm p^2. The 6 is computed in a similar way to Lemma 1 and gives an upper bound for the contribution of primes above 3. ∎

Altogether we get the following upper bound for the number of S_4-fields associated to a given triple (a, b, c):
$$3 \cdot \frac{3^{r_1} - 1}{3 - 1} (2^{r_2} - 1) \le \frac{3}{2} \cdot 9 \cdot 2^6 3^{\mathrm{rk}_3(\mathrm{Cl}_k)} 2^{\mathrm{rk}_3(\mathrm{Cl}_M)} 3^{\omega(b)} 8^{\omega(c)}, \tag{2}$$
where $r_1 = \mathrm{rk}_3(\mathrm{Cl}_k) + \omega(b) + 2$ and $r_2 = \mathrm{rk}_3(\mathrm{Cl}_M) + 3\omega(c) + 6$.

The following theorem relates the 3-parts of the class groups of k and M.

THEOREM 1 (Gerth III). *Let $M/\mathbb{Q}$ be a non-cyclic cubic extension and denote by L the normal closure of M and by k the unique quadratic subfield of L. Then*:

(i) *If L/k is unramified, then* $\mathrm{rk}_3(\mathrm{Cl}_M) = \mathrm{rk}_3(\mathrm{Cl}_k) - 1$.
(ii) $\mathrm{rk}_3(\mathrm{Cl}_M) = \mathrm{rk}_3(\mathrm{Cl}_k) + t - 1 - z - y$, *where $y \le t-1$ and t is the number of prime ideals of $\mathcal{O}_k$ which ramify in L. Furthermore we have $0 \le z \le u$ where u is the number of primes which are totally ramified in M but split in k.*
(iii) $\mathrm{rk}_3(\mathrm{Cl}_M) \ge \mathrm{rk}_3(\mathrm{Cl}_k) - u$.

Proof. The first part is Theorem 3.4 in [Ger76]. The second part is Theorem 3.5 in that paper. The last part is an immediate consequence. ∎

Since we are only interested in the asymptotic behaviour we can ignore ramification at 2 and 3. Therefore we define $S := \{2,3\}$ and a^S to be the largest number dividing a which is coprime to S. Using this we easily see that $d_M^S = a^S(b^S)^2$, where M is one of the cubic extensions constructed above. Using Theorem 1 we get the following estimate for $3^{\mathrm{rk}_3(\mathrm{Cl}_k)}2^{\mathrm{rk}_3(\mathrm{Cl}_M)}$.

LEMMA 4. *Let M, k be the fields defined before. Then there exists a constant $C > 0$ such that*

$$3^{\mathrm{rk}_3(\mathrm{Cl}_k)}2^{\mathrm{rk}_2(\mathrm{Cl}_M)} \le Ca^{1/2}b\log(ab^2)^2 3^{\omega(b)}.$$

Proof. Theorem 1 shows $\mathrm{rk}_3(\mathrm{Cl}_M) \ge \mathrm{rk}_3(\mathrm{Cl}_k) - \omega(b)$. Therefore we get

$$3^{\mathrm{rk}_3(\mathrm{Cl}_k)}2^{\mathrm{rk}_2(\mathrm{Cl}_M)} \le 3^{\mathrm{rk}_3(\mathrm{Cl}_M)}3^{\omega(b)}2^{\mathrm{rk}_2(\mathrm{Cl}_M)} \le 3^{\omega(b)}|\mathrm{Cl}_M|.$$

Using Lemma 2 and the fact that $d_M^S = (ab^2)^S$ differs from d_M by a quantity which can be bounded by a constant we get the desired bound. ∎

Combining Lemma 4 and (2) we deduce the following corollary.

COROLLARY 1. *The number of elements of the fibre $\Psi^{-1}(a,b,c)$ is bounded by*

$$3^3 2^5 Ca^{1/2}b\log(ab^2)^2 9^{\omega(b)}8^{\omega(c)}.$$

3. Upper bounds for quartic S_4-extensions with given discriminant. In this section we prove an upper bound for the number of quartic S_4-extensions with given discriminant. In order to do this we need to compute the discriminant d_K using the triple (a,b,c). In a second step we determine how many triples may lead to the same discriminant.

Let us assume that we are given a field $K \in \mathcal{K}$ with $\Psi(K) = (a,b,c)$ ramified at p. Assuming $p \ne 2,3$ we can compute the cycle shape of a generator of the cyclic inertia group at p in the degree 4 representation of S_4. Here the cycle shape means the lengths of the cycles if we decompose a group element into disjoint cycles. Using local theory we get for primes $p > 3$ the following identities, where v_p denotes the ordinary p-valuation:

	Cycle shape	$v_p(d_K)$
$p \mid a,\ p \nmid bc$	$1^2 2$	1
$p \mid a,\ p \mid c,\ p \nmid b$	4	3
$p \mid b,\ p \nmid ac$	13	2
$p \mid c,\ p \nmid ab$	2^2	2

The other cases cannot occur since in these cases the inertia group would not be cyclic. The cases $p = 2$ and $p = 3$ can be handled by analyzing the local Galois groups. We still use the definition of a^S for $S := \{2, 3\}$ from the preceding section and get

$$d_K^S = a^S (b^S)^2 (c^S)^2.$$

The contribution of the primes 2 and 3 is bounded by a constant factor. Therefore we ignore these primes in the following.

Using the results of the preceding section it remains to count the number of triples (a, b, c) which may lead to the same discriminant. In the following let d be the discriminant of a quartic S_4-extension.

THEOREM 2. *Let $d = 2^{e_2} 3^{e_3} d_1 d_2^2 d_3^3$ be such that $6 d_1 d_2 d_3$ is squarefree. Then the number of S_4-fields with discriminant d is bounded above by*

(i) $\widetilde{C} (d_1 d_3)^{1/2} d_2 \log(d_1 d_3 d_2^2)^2 18^{\omega(d_2)} 8^{\omega(d_3)}$ *for a suitable* $\widetilde{C} > 0$,
(ii) $O_\varepsilon(d^{1/2+\varepsilon})$ *for all* $\varepsilon > 0$.

Proof. By the above discussion all fields $K/\mathbb{Q}$ with $\Psi(K) = (a, b, c)$ have the properties

$$a^S = d_1 d_3, \qquad d_3 \mid c^S, \qquad (bc)^S = d_2 d_3.$$

Therefore we have $2^{\omega(d_2)}$ possibilities for choosing b^S. The number of possibilities for the 2- and the 3-part can be bounded by a constant. By Corollary 1 the worst case is when $b^S = d_2$ and therefore, for some computable constant $\widetilde{C} > 0$, we get

$$\widetilde{C} 2^{\omega(d_2)} (d_1 d_3)^{1/2} d_2 \log(d_1 d_3 d_2^2)^2 9^{\omega(d_2)} 8^{\omega(d_3)}$$

as an upper bound. For the second statement we write $x^{\omega(d)} = O(d^\varepsilon)$ for a given number x and get the desired result. ∎

REMARK 1. For squarefree discriminants d we can derive the better upper bound $O(d^{1/2} \log(d)^2)$.

We can combine Theorem 2 with well known results to get bounds for degree 4 fields.

THEOREM 3. *The number of degree 4 fields of given discriminant d is bounded above by $O_\varepsilon(d^{1/2+\varepsilon})$ for all $\varepsilon > 0$.*

Proof. Using the theorem of Kronecker–Weber we easily deduce that the number of fields with Abelian Galois group is bounded by $O_\varepsilon(d^\varepsilon)$ for all $\varepsilon > 0$. Since D_4-fields can be constructed by quadratic extensions over quadratic extensions and the 2-torsion part of the class group can be easily controlled, we get the same result for D_4-extensions.

For A_4-extensions we use the same approach as in the S_4-case. The main difference is that we have only one step where we need to consider class groups. This gives $O_\varepsilon(d^{1/2+\varepsilon})$ for the number of such extensions with given discriminant d. Using more advanced methods [MV02] this number can be reduced to $O_\varepsilon(d^{1/3+\varepsilon})$. ∎

4. Upper bounds for the dimension of the space of octahedral modular forms of given conductor. In this section we give upper bounds for the dimension of the space of octahedral modular forms of weight 1. Denote by $G_{\mathbb{Q}}$ the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Suppose we are given a quartic S_4-extension $K/\mathbb{Q}$ which gives rise to a projective representation $\widetilde{\varrho} : G_{\mathbb{Q}} \to \mathrm{PGL}_2(\mathbb{C})$. The *conductor* of this projective representation is defined to be the product of the local conductors of $\varrho | G_{\overline{\mathbb{Q}}_p} : G_{\overline{\mathbb{Q}}_p} \to \mathrm{PGL}_2(\mathbb{C})$ which is the minimal p-power of a so-called local lift (see e.g. [Ser77, §6] or [Won99] for more details).

In this section we count S_4-extensions using the above-defined conductor. A prime p divides the conductor if and only if p divides the discriminant. To simplify all computations we ignore the contribution of the 2- and 3-part of the conductor. All other (tamely) ramified primes have the property that p exactly divides the conductor when the local Galois group is cyclic. Otherwise the local Galois group is dihedral and p^2 exactly divides the conductor [Won99, Prop. 1, p. 144].

To each projective representation with image S_4 we can associate an octahedral modular form of the same conductor. This means that we get the corresponding bounds for the modular forms when we compute the bounds for the number of projective representations (see e.g. [Duk95, Won99] for more details).

In order to use the results of Section 2 we need to compute the conductor of the associated modular form only using the triple (a, b, c). Similarly to the discriminant case we can do all computations locally. In the discriminant case it was only important to know the inertia group. Now it is important to know the decomposition group. Let $p > 3$ be a divisor of abc. Then p exactly divides the conductor if the decomposition group is cyclic. In the following table we collect the information we get (for $p > 3$) using the prime ideal factorization

$$p\mathcal{O}_K = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}.$$

We remark that some cases can be distinguished by congruence conditions. In the last column we place the letters which are divisible by p. The information $v_p(d)$ on the discriminant is not needed in this section.

	D_p	I_p	$v_p(N)$	$v_p(d)$	$p \equiv$	$p \mid$
$\mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$	C_2	C_2	1	1		a
$\mathfrak{p}_1^2\mathfrak{p}_2$	$C_2 \times C_2$	C_2	2	1		a
$\mathfrak{p}_1^2$	$C_2 \times C_2$ or C_4	C_2	2 or 1	2		c
$\mathfrak{p}_1^2\mathfrak{p}_2^2$	$C_2 \times C_2$ or C_2	C_2	2 or 1	2		c
$\mathfrak{p}_1^4$	D_4	C_4	2	3	3 mod 4	a, c
$\mathfrak{p}_1^4$	C_4	C_4	1	3	1 mod 4	a, c
$\mathfrak{p}_1^3\mathfrak{p}_2$	C_3	C_3	1	2	1 mod 3	b
$\mathfrak{p}_1^3\mathfrak{p}_2$	D_3	C_3	2	2	2 mod 3	b

Let $K/\mathbb{Q}$ be a quartic S_4-extension with associated triple (a, b, c) and conductor N. Then we write

$$a = a_1a_2, \quad b = b_1b_2, \quad c = c_0c_1c_2,$$

where $c_0 := \gcd(a, c)$ is such that

$$N^S = (a_1a_2^2b_1b_2^2c_1c_2^2)^S.$$

Since $\gcd(b, ac)^S = 1$ we easily see that $a_1^S, a_2^S, b_1^S, b_2^S, c_1^S, c_2^S$ are pairwise coprime. Using the above table we know that b_i is (up to the 3-part) exactly divisible by the primes dividing b which are congruent to i mod 3 $(i = 1, 2)$.

Theorem 4. *Let $N = 2^{n_2}3_3^{n}N_{1,1}N_{1,2}N_2^2$ be such that $6N_{1,1}N_{1,2}N_2$ is squarefree. Furthermore we assume that $p \mid N_{1,i}$ if and only if $p \equiv i \bmod 3$ $(i = 1, 2)$. Then the number of S_4-fields of given conductor N is bounded above by*

$$C54^{\omega(N)}N_{1,1}N_{1,2}^{1/2}N_2 \log(N)^2$$

for a suitable $C > 0$.

Proof. We have $3^{\omega(N)}$ possibilities to partition the primes into three sets corresponding to a, b, c. Furthermore we have at most $2^{\omega(N)}$ possibilities for c_0. Using Corollary 1 we have the worst case when b is large. Primes dividing $N_{1,2}$ cannot divide b. Here we get the worst case when these primes divide a. Therefore we have an upper bound

$$\widetilde{C}3^{\omega(N)}2^{\omega(N)}N_{1,1}N_{1,2}^{1/2}N_2 \log(N_{1,2}N_{1,1}^2N_2^2)^2 9^{\omega(N)}.$$

We easily get the desired result. ∎

To get good estimates for the dimension of the space of octahedral forms with given conductor we have to avoid the situation when b_1 is large. Using this we can derive the following corollaries.

COROLLARY 2. *Let p be a prime. Then the dimension of the space of octahedral modular forms of weight 1 and conductor p or p^2 is bounded above by $O(p^{1/2}\log(p)^2)$.*

Proof. The quadratic subextension must be ramified at at least one prime. Therefore $p \mid a$ for all possible triples. ∎

COROLLARY 3. *Assume that all primes which exactly divide N are congruent to $2 \bmod 3$. Then the dimension of the space of octahedral forms of weight 1 and conductor N is bounded above by $O(N^{1/2+\varepsilon})$ for all $\varepsilon > 0$.*

Proof. We have $N_{1,1} = 1$ and the assertion follows. ∎

This improves the bound $O(N^{4/5+\varepsilon})$ given in [MV02]. We remark that in the case that b_1 resp. $N_{1,1}$ is large we only get the trivial linear bound using our method.

Acknowledgments. I thank Karim Belabas and Gunter Malle for fruitful discussions and for reading a preliminary version of the paper.

References

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

[Bel04] K. Belabas, *Paramétrisation de structures algébriques et densité de discriminants, d'après Bhargava*, Séminaire Bourbaki 56 (2004), no. 935.

[Bha02] M. Bhargava, *Gauss composition and generalizations*, in: Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci. 2369, Springer, Berlin, 2002, 1–8.

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

[FK03] C. Fieker and J. Klüners, *Minimal discriminants for fields with small Frobenius groups as Galois groups*, J. Number Theory 99 (2003), 318–337.

[Ger76] F. Gerth III, *Ranks of 3-class groups of non-Galois cubic fields*, Acta Arith. 30 (1976), 307–322.

[HV04] H. A. Helfgott and A. Venkatesh, *Integral points on elliptic curves and 3-torsion in class groups*, J. Amer. Math. Soc., to appear.

[HPP03] F. Hess, S. Pauli, M. E. Pohst, *Computing the multiplicative group of residue class rings*, Math. Comp. 72 (2003), no. 243, 1531–1548.

[MV02] Ph. Michel and A. Venkatesh, *On the dimension of the space of cusp forms associated to 2-dimensional complex Galois representations*, Internat. Math. Res. Notices 2002, no. 38, 2021–2027.

[Nar90] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 2nd ed., PWN, Warszawa, and Springer, Berlin, 1990.

[Pie05] L. B. Pierce, *The* 3*-part of class numbers of quadratic fields*, J. London Math. Soc. (2) 71 (2005), 579–598.

[Ser77] J.-P. Serre, *Modular forms of weight one and Galois representations*, in: Algebraic Number Fields: L-functions and Galois Properties (Durham, 1975), Academic Press, London, 1977, 193–268.

[Ser95] —, *Local Fields*, 2nd ed., Springer, New York, 1995.

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

Fachbereich Mathematik/Informatik
Universität Kassel
Heinrich-Plett-Str. 40
34132 Kassel, Germany
E-mail: klueners@mathematik.uni-kassel.de

Received on 4.8.2005 (5048)