MATHEMATICS OF COMPUTATION
VOLUME 58, NUMBER 198
APRIL 1992, PAGES 831–847

MULTIPLICITIES OF DIHEDRAL DISCRIMINANTS

DANIEL C. MAYER

Dedicated to the memory of Helmut Hasse

ABSTRACT. Given the discriminant d_k of a quadratic field k, the number of cyclic relative extensions $N|k$ of fixed odd prime degree p with dihedral absolute Galois group of order $2p$, which share a common conductor f, is called the multiplicity of the dihedral discriminant $d_N = f^{2(p-1)}d_k^p$. In this paper, general formulas for multiplicities of dihedral discriminants are derived by analyzing the p-rank of the ring class group mod f of k. For the special case $p = 3$, $d_k = -3$, an elementary proof is given additionally. The theory is illustrated by a discussion of all known discriminants of multiplicity ≥ 5 of totally real and complex cubic fields.

INTRODUCTION

Let p be an odd prime and $K|\mathbb{Q}$ a cyclic extension of degree p. Then it is well known [9, 15, 7] that the conductor of K must have the form $f = p^e \cdot q_1 \cdots q_t$, where $e = 0$ or $e = 2$, $t \geq 0$, and the q_i are pairwise distinct rational primes satisfying $q_i \equiv 1 \pmod{p}$ for $i = 1, \ldots, t$. The discriminant of K is just a power of the conductor, $d_K = f^{p-1}$. If, for any positive integer f, the number of cyclic extensions $K|\mathbb{Q}$ of degree p which share the same conductor f is denoted by $m(f)$, then

$$\sum_{f'|f} m(f') = \frac{1}{p-1}(p^\rho - 1),$$

where $\rho = \dim_{\mathbb{F}_p}(\mathbb{Q}^\times(f)/\mathbb{Q}_f^\times \cdot \mathbb{Q}^\times(f)^p) = \dim_{\mathbb{F}_p}(\mathrm{Syl}_p\, U(\mathbb{Z}/f\mathbb{Z}) \otimes_{\mathbb{Z}_p} \mathbb{F}_p) = t + w$ with $\mathbb{Q}^\times(f) = \{r \in \mathbb{Q}^\times \mid (r, f) = 1\}$, $\mathbb{Q}_f^\times = \{r \in \mathbb{Q}^\times \mid r \equiv 1 \pmod{^\times f}\}$, and $w = \frac{1}{2}e$. Moebius inversion yields an explicit formula for $m(f)$:

$$m(p^e \cdot q_1 \cdots q_t) = (p-1)^{t+w-1}.$$

It is the aim of the present paper to establish similar formulas for multiplicities of discriminants in the case of non-Galois extensions $L|\mathbb{Q}$ of degree p with dihedral normal closure N of degree $2p$. For the sake of illustration, the formulas are applied to discriminants with multiplicities up to 16 of non-Galois

Received December 10, 1990; revised April 5, 1991.
1991 *Mathematics Subject Classification.* Primary 11R20, 11R11, 11R16.
Key words and phrases. Dihedral fields, quadratic ring class groups, cubic fields.
Research supported by the Austrian Science Foundation, Project Nr. J0497-PHY.

0025-5718/92 $1.00 + $.25 per page

cubic fields which occur in the most extensive recent numerical tables [10, 5, 11].

1. Cubic discriminants

Assume that k is a fixed quadratic field with discriminant d_k. If $N|k$ is a cyclic cubic relative extension with conductor f and with absolute Galois group $\mathrm{Gal}(N|\mathbb{Q}) \simeq S_3$, the symmetric group on three symbols, then [8, p. 578] f must have the form

$$f = 3^e \cdot q_1 \cdots q_t$$

with $0 \leq e \leq 2$, $t \geq 0$, and pairwise distinct rational primes $q_i \neq 3$ satisfying $q_i \equiv (\frac{d_k}{q_i})$ (mod 3) for $i = 1, \ldots, t$. Furthermore, the 3-exponent e is restricted to the values 0, 2 if $d_k \equiv \pm 1 \pmod 3$, and to the values 0, 1 if $d_k \equiv 3 \pmod 9$, but no restrictions arise for $d_k \equiv -3 \pmod 9$. An integer f of this form will be called an *admissible conductor* for the quadratic discriminant d_k.

For any positive integer f, define the *multiplicity* $m(d_k, f)$ of f with respect to d_k to be the number of nonconjugate cubic fields $L|\mathbb{Q}$ with coinciding discriminant $d_L = f^2 \cdot d_k$. Then the following general formula for the recursive determination of multiplicities of cubic discriminants holds. This result will be proved in a more general context in §3.

Theorem 1.1. *Let $f = 3^e \cdot q_1 \cdots q_t$ be an admissible conductor for the quadratic field k with discriminant d_k and 3-class rank ρ. Then*

$$\sum_{f'|f} m(d_k, f') = \frac{1}{2}(3^{\rho+t+w-\delta} - 1) ,$$

where the sum runs over all divisors f' of f. Here,

$$w = \begin{cases} 0 & \text{if } e = 0, \\ 2 & \text{if } e = 2 \text{ and } d_k \equiv -3 \pmod 9, \\ 1 & \text{otherwise}, \end{cases}$$

and $\delta = \dim_{\mathbb{F}_3}(I_{k,3}(f)/I_{k,3}(f) \cap (\mathbb{Q}^\times(f) k_f^\times k^\times(f)^3))$, where $k^\times(f)$ (resp. $\mathbb{Q}^\times(f)$) denotes the numbers in $k^\times$ (resp. $\mathbb{Q}^\times$) which are coprime to f, $k_f^\times = \{\gamma \in k^\times \mid \gamma \equiv 1 \pmod{{}^\times f}\}$ is the group of generators of the ray $\bmod f$ of k, and $I_{k,3}(f) = I_{k,3} \cap k^\times(f)$ with the group $I_{k,3}$ of generators $\alpha \in k^\times$ of all principal ideals $\alpha\mathcal{O}_k$ which are cubes of ideals of k.

2. Pure cubic discriminants

First, the complete solution of the multiplicity problem for the special case of pure cubic discriminants is obtained in a totally elementary way with the aid of the following well-known relationship [4] between the normalized radicand $D = m \cdot n^2$ of a pure cubic field $L = \mathbb{Q}(\sqrt[3]{D})$, where $m > n > 0$ are squarefree coprime integers, and the conductor f of the corresponding relative extension $N|k$,

$$f = \begin{cases} 3mn & \text{if } D \not\equiv \pm 1 \pmod 9 \text{ (field of Dedekind's 1st kind)}, \\ mn & \text{if } D \equiv \pm 1 \pmod 9 \text{ (field of Dedekind's 2nd kind)}. \end{cases}$$

Theorem 2.1. *Let* $f = 3^e \cdot q_1 \cdots q_t > 1$ *be an admissible conductor for the special quadratic discriminant* $d_k = -3$, *i.e.,* $0 \le e \le 2$, $t \ge 0$, *and* $q_i \ne 3$ *are arbitrary rational primes for* $i = 1, \dots, t$. *Put*

$$u = \#\{1 \le i \le t \mid q_i \equiv \pm 1 \pmod 9\},$$
$$v = \#\{1 \le i \le t \mid q_i \equiv \pm 2, \pm 4 \pmod 9\}.$$

Then the multiplicity $m(f) := m(-3, f)$ *of the pure cubic discriminant* $-3 \cdot f^2$ *is given by*

$$m(3^e \cdot q_1 \cdots q_t) = \begin{cases} 2^t & \text{if } e = 2, \\ 2^u \cdot X_v & \text{if } e = 1, \\ 2^u \cdot X_{v-1} & \text{if } e = 0, \end{cases}$$

where $X_j = \frac{1}{3}(2^j + (-1)^{j+1})$ *for all* $j \ge -1$.

Moreover, the multiplicities of conductors with 3*-exponents* $e = 0, 1$ *satisfy the relation*

$$m(q_1 \cdots q_t) + m(3 \cdot q_1 \cdots q_t) = 2^{t-1}.$$

Proof. To see that all claimed conductors are really admissible for $d_k = -3$, observe that $d_k \equiv -3 \pmod 9$ and that the condition $q \equiv (\frac{d_k}{q}) \pmod 3$ is satisfied by every prime q.

First, the case $e = 2$ is treated separately. The relation $f = 3^2 \cdot q_1 \cdots q_t$ is equivalent to $f = 3mn$, $3 \mid mn$, and thus also to $D \equiv 0 \pmod 3$. In this case, there are 2^{t+1} choices for the exponent systems $1 \le w_0, w_1, \dots, w_t \le 2$ in cubefree radicands $D = 3^{w_0} \cdot q_1^{w_1} \cdots q_t^{w_t}$ which all share the same value of $mn = 3 \cdot q_1 \cdots q_t$. But only one of the two systems $(w_0, \dots, w_t)$ and $(3 - w_0, \dots, 3 - w_t)$ belongs to a normalized radicand. Hence,

$$m(3^2 \cdot q_1 \cdots q_t) = \tfrac{1}{2} 2^{t+1} = 2^t.$$

Second, the cases $e = 1$ and $e = 0$ are investigated simultaneously. The relation $f = 3 \cdot q_1 \cdots q_t$ is equivalent to $f = 3mn$, $3 \nmid mn$, and further to $D \equiv \pm 2, \pm 4 \pmod 9$, whereas $f = q_1 \cdots q_t$ is equivalent to $f = mn$, $3 \nmid mn$, and also to $D \equiv \pm 1 \pmod 9$. In both cases, there are 2^t choices for exponents $1 \le w_1, \dots, w_t \le 2$ in cubefree radicands $D = q_1^{w_1} \cdots q_t^{w_t}$ which all share the same value of $mn = q_1 \cdots q_t$, but some of them ($D \equiv \pm 1 \pmod 9$) give rise to conductor $f = mn$ and the others ($D \equiv \pm 2, \pm 4 \pmod 9$) to conductor $f = 3mn$. Again, only one of the two systems $(w_1, \dots, w_t)$ and $(3 - w_1, \dots, 3 - w_t)$ belongs to a normalized radicand. (Both, the normalized and the nonnormalized radicand, are of the same Dedekind kind.) Therefore,

$$m(q_1 \cdots q_t) + m(3 \cdot q_1 \cdots q_t) = \tfrac{1}{2} 2^t = 2^{t-1}.$$

To separate these two multiplicities, it is convenient to fix a value $u \ge 0$ of the number of prime divisors $q \equiv \pm 1 \pmod 9$ of D and to argue by induction with respect to the number $v \ge 0$ of prime divisors $q \equiv \pm 2, \pm 4 \pmod 9$ of D. Obviously, $u + v = t$.

Induction start, $v = 0, 1$:

In the case $v = 0$, we have $mn = q_1 \cdots q_u$ with $u \ge 1$ and $D \equiv \pm 1 \pmod 9$, whence

$$Y_{-1} := m(q_1 \cdots q_u) = 2^{u-1},$$
$$Y_0 := m(3 \cdot q_1 \cdots q_u) = 0.$$

In the case $v = 1$, we have $mn = q_1 \cdots q_u \cdot q_{u+1}$ and $D \equiv \pm 2, \pm 4 \pmod 9$, whence

$$m(q_1 \cdots q_u \cdot q_{u+1}) = 0 = Y_0,$$
$$Y_1 := m(3 \cdot q_1 \cdots q_u \cdot q_{u+1}) = 2^u.$$

Induction step, $v \to v+1$:

If the new prime factor $q_{u+v+1} \equiv \pm 2, \pm 4 \pmod 9$ and its square are multiplied by a radicand $D \equiv \pm 1 \pmod 9$, then there are generated two new radicands $D \cdot q_{u+v+1}^{w_{u+v+1}} \equiv \pm 2, \pm 4 \pmod 9$ with $1 \le w_{u+v+1} \le 2$. However, if they are multiplied by a radicand $D \equiv \pm 2, \pm 4 \pmod 9$, then one of the two new radicands is congruent $\pm 1 \pmod 9$ (the one, where $q_{u+v+1}^{w_{u+v+1}}$ represents the square of D in the group $U(\mathbb{Z}/9\mathbb{Z})/\{\pm 1\} \simeq C(3)$) and the other is congruent $\pm 2, \pm 4 \pmod 9$. Thus,

$$m(q_1 \cdots q_{u+v+1}) = m(3 \cdot q_1 \cdots q_{u+v}) =: Y_v,$$
$$\begin{aligned} Y_{v+1} := m(3 \cdot q_1 \cdots q_{u+v+1}) &= m(3 \cdot q_1 \cdots q_{u+v}) + 2 \cdot m(q_1 \cdots q_{u+v}) \\ &= Y_v + 2Y_{v-1}. \end{aligned}$$

Consequently, the numbers Y_j $(j \ge -1)$ satisfy a binary linear recursion, $Y_{j+1} = Y_j + 2Y_{j-1}$ for $j \ge 0$, with initial values $Y_{-1} = 2^{u-1}$ and $Y_0 = 0$. This recursion can be solved by diagonalization of the corresponding matrix M in the equation

$$\begin{pmatrix} Y_{j+1} \\ Y_j \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} Y_j \\ Y_{j-1} \end{pmatrix}.$$

The characteristic polynomial of M is (denoting by I the identity matrix)

$$\det(x \cdot I - M) = x^2 - x - 2 = (x+1) \cdot (x-2).$$

The eigenspaces of M with respect to the eigenvalues -1 and 2 are

$$\ker(M + I) = \mathbb{Q} \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \qquad \ker(M - 2 \cdot I) = \mathbb{Q} \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix},$$

and M becomes diagonal under the transformation

$$T^{-1} \cdot M \cdot T = \frac{1}{3} \begin{pmatrix} 1 & -2 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 2 \end{pmatrix} := \Delta.$$

Therefore, the solution of the recursion can be represented in the form

$$\begin{aligned} \begin{pmatrix} Y_j \\ Y_{j-1} \end{pmatrix} = M^j \cdot \begin{pmatrix} Y_0 \\ Y_{-1} \end{pmatrix} &= T \cdot \Delta^j \cdot T^{-1} \cdot \begin{pmatrix} Y_0 \\ Y_{-1} \end{pmatrix} \\ &= \frac{1}{3} 2^u \begin{pmatrix} (-1)^{j+1} + 2^j \\ (-1)^j + 2^{j-1} \end{pmatrix} \quad \text{for } j \ge 0. \end{aligned}$$

Hence, the solution is $Y_j = 2^u \cdot X_j$ with $X_j := \frac{1}{3}(2^j + (-1)^{j+1})$ for all $j \ge -1$. □

Remark. The proof of Theorem 2.1 used a very special elementary technique which cannot be applied to other types of cubic fields. In the next section, this result will be rederived as a particular instance of a much more general formula, which is deduced by completely different methods, using ring class groups of quadratic number fields.

Examples. As an application, the minimal occurrences of some higher multiplicities of pure cubic discriminants are determined. The first three cases appear in tables of complex cubic fields [1, 5, 12] which are ordered by discriminants. The further ones are constructed by means of Theorem 2.1, taking the smallest possible prime factors. These examples show that the normalized radicands associated with a fixed discriminant of higher multiplicity are spread rather widely in a table of pure cubic fields which is ordered by radicands, such as [11].

1. $m(f) = 2$ for $f = 3^2 \cdot 2$, $d_L = -972$, occurs in [1], with associated radicands $D = 6, 12$, and $e = 2$, $u = 0$, $v = 1$.
2. $m(f) = 4$ for $f = 3^2 \cdot 2 \cdot 5$, $d_L = -24\,300$, occurs in [12], with associated radicands $D = 30, 60, 90, 150$, and $e = 2$, $u = 0$, $v = 2$.
3. $m(f) = 3$ for $f = 3 \cdot 2 \cdot 5 \cdot 7$, $d_L = -132\,300$, occurs in [5], with associated radicands $D = 70, 140, 490$, and $e = 1$, $u = 0$, $v = 3$.
4. $m(f) = 8$ for $f = 3^2 \cdot 2 \cdot 5 \cdot 7$, $d_L = -1\,190\,700$, occurs in [11], with associated radicands $D = 210, 420, 630, 1050, 1260, 1470, 2100, 2940$, and $e = 2$, $u = 0$, $v = 3$.
5. $m(f) = 5$ for $f = 3 \cdot 2 \cdot 5 \cdot 7 \cdot 11$, $d_L = -16\,008\,300$, occurs in [11], with associated radicands $D = 770, 3850, 7700, 10780, 16940$, and $e = 1$, $u = 0$, $v = 4$.
6. $m(f) = 6$ for $f = 3 \cdot 2 \cdot 5 \cdot 7 \cdot 17$, $d_L = -38\,234\,700$, occurs in [11], with associated radicands $D = 1190, 2380, 8330, 11900, 20230, 40460$, and $e = 1$, $u = 1$, $v = 3$.
7. However, $m(f) = 7$ will never occur, since 7 is not a member of the sequence $(X_j)_{j \geq -1}$ in Theorem 2.1. The same is true for $m(f) = 9, 13, 14, 15$.
8. $m(f) = 16$ for $f = 3^2 \cdot 2 \cdot 5 \cdot 7 \cdot 11$, $d_L = -144\,074\,700$, occurs in [11], with associated radicands $D = 2310, 4620, 6930, 11550, 13860, 16170, 23100, 25410, 32340, 34650, 48510, 50820, 69300, 76230, 80850, 97020$, and $e = 2$, $u = 0$, $v = 4$.
9. $m(f) = 11$ for $f = 3 \cdot 2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$, $d_L = -2\,705\,402\,700$, with associated radicands $D = 10010, 20020, 70070, 100100, 110110, 260260, 350350, 550550, 650650, 700700, 910910$, and $e = 1$, $u = 0$, $v = 5$.
10. $m(f) = 10$ for $f = 3 \cdot 2 \cdot 5 \cdot 7 \cdot 11 \cdot 17$, $d_L = -4\,626\,398\,700$, with associated radicands $D = 13090, 65450, 130900, 183260, 222530, 287980, 458150, 719950, 1007930, 1112650$, and $e = 1$, $u = 1$, $v = 4$.
11. $m(f) = 12$ for $f = 3 \cdot 2 \cdot 5 \cdot 7 \cdot 17 \cdot 19$, $d_L = -13\,802\,726\,700$, with associated radicands $D = 22610, 45220, 158270, 226100, 384370, 429590, 768740, 791350, 859180, 1582700, 2690590, 3007130$, and $e = 1$, $u = 2$, $v = 3$.

3. Dihedral discriminants

As before, assume that k is a fixed quadratic field with discriminant d_k. With p an odd rational prime, let $N|k$ be a cyclic relative extension of degree p with conductor f and absolute Galois group $\mathrm{Gal}(N|\mathbb{Q}) \simeq D_p$, the dihedral group of order $2p$. Then f is a rational integer and [2] must have the form

$$f = p^e \cdot q_1 \cdots q_t$$

with $0 \leq e \leq 2$, $t \geq 0$, and pairwise distinct rational primes $q_i \neq p$ satisfying $q_i \equiv (\frac{d_k}{q_i}) \pmod{p}$ for $i = 1, \ldots, t$. Furthermore, the p-exponent e is restricted to the values $0, 2$ if p is unramified in k, and to the values $0, 1$ if $p \mid d_k$, except for the special configuration where $p = 3$ and $d_k \equiv -3 \pmod{9}$. An integer f of this form will be called a *p-admissible conductor* for the quadratic discriminant d_k.

For any positive integer f, define the *p-multiplicity* $m_p(d_k, f)$ of f with respect to d_k to be the number of nonisomorphic fields $L|\mathbb{Q}$ of degree p sharing the same discriminant $d_L = f^{p-1} \cdot d_k^{(p-1)/2}$. By the translation theorem of Galois theory, $m_p(d_k, f)$ is also the number of cyclic extensions $N|k$ of degree p with absolute group $\mathrm{Gal}(N|\mathbb{Q}) \simeq D_p$ sharing the common conductor f.

Remark. If f is not a p-admissible conductor for d_k, then certainly $m_p(d_k, f) = 0$. But on the other hand, $m_p(d_k, f)$ may be zero even for a p-admissible conductor f for d_k, as will be shown for infinite families of fields in Corollaries 3.2 and 3.3.

Denote by $\mathscr{I}_k(f)$ the group of (fractional) ideals of k coprime to f, and by $\mathscr{R}_{k,f} = \{\alpha\mathscr{O}_k \mid \alpha \in \mathbb{Q}^\times(f) \cdot k_f^\times\}$ the so-called *ring* mod f of k, where $\mathbb{Q}^\times(f)$ denotes the numbers in $\mathbb{Q}^\times$ which are coprime to f, and $k_f^\times = \{\gamma \in k^\times \mid \gamma \equiv 1 \pmod{{}^\times f}\}$ is the group of generators of the ray mod f of k. Then, by the Artin reciprocity law of class field theory [8], $m_p(d_k, f)$ can be interpreted as the number of subgroups $\mathscr{H}$ of index p of $\mathscr{I}_k(f)$ which contain $\mathscr{R}_{k,f}$ but not $\mathscr{R}_{k,f'}$ for any proper divisor $f'|f$, $f' \neq f$. With the aid of this fact, the following formula for the recursive determination of multiplicities of dihedral discriminants can be derived.

Theorem 3.1. *Let $f = p^e \cdot q_1 \cdots q_t$ be a p-admissible conductor for a given quadratic field k with discriminant d_k and with p-class rank $\rho = \rho_k(p)$. Then*

$$\sum_{f'|f} m_p(d_k, f') = \frac{1}{p-1}(p^{\rho+t+w-\delta} - 1),$$

where the sum runs over all divisors f' of f. Here,

$$w = \begin{cases} 0 & \text{if } e = 0, \\ 2 & \text{if } e = 2,\ p = 3,\ d_k \equiv -3 \pmod{9}, \\ 1 & \text{otherwise}, \end{cases}$$

and $\delta = \delta(f) = \dim_{\mathbb{F}_p}(I_{k,p}(f)/I_{k,p}(f) \cap (\mathbb{Q}^\times(f)k_f^\times k^\times(f)^p))$, where the numbers in $k^\times$ which are coprime to f are denoted by $k^\times(f)$, and $I_{k,p}(f) = I_{k,p} \cap k^\times(f)$ with the group $I_{k,p}$ of generators $\alpha \in k^\times$ of all principal ideals $\alpha\mathscr{O}_k$ which are pth powers of ideals of k.

Proof. Since the ring class group mod f of k, $\mathscr{I}_k(f)/\mathscr{R}_{k,f}$, is an abelian group, its p-elementary subgroup is isomorphic to $\mathscr{I}_k(f)/(\mathscr{R}_{k,f} \cdot \mathscr{I}_k(f)^p)$. Hence, any subgroup $\mathscr{H}$ of index p in $\mathscr{I}_k(f)$ which contains $\mathscr{R}_{k,f}$ must in fact be an intermediate group $\mathscr{R}_{k,f} \cdot \mathscr{I}_k(f)^p < \mathscr{H} < \mathscr{I}_k(f)$. Therefore,

$$\sum_{f'|f} m_p(d_k, f') = \#\{\mathscr{H} < \mathscr{I}_k(f) \mid (\mathscr{I}_k(f) : \mathscr{H}) = p,\ \mathscr{R}_{k,f} \cdot \mathscr{I}_k(f)^p < \mathscr{H}\}$$

is exactly the number of the hyperplanes (subspaces of codimension 1) of the p-elementary ring class group mod f of k, viewed as a vector space over the finite field $\mathbb{F}_p$. But this number equals $\frac{1}{p-1}(p^{\rho'}-1)$, where $\rho' = \dim_{\mathbb{F}_p}(\mathscr{I}_k(f)/\mathscr{R}_{k,f}\cdot\mathscr{I}_k(f)^p)$ is the p-rank of $\mathscr{I}_k(f)/\mathscr{R}_{k,f}$.

If $\mathscr{P}_k(f) = \mathscr{P}_k \cap \mathscr{I}_k(f)$ denotes the principal ideals of k coprime to f, then the factorization relation of elementary abelian p-groups,

$$\mathscr{I}_k(f)/\mathscr{P}_k(f)\cdot\mathscr{I}_k(f)^p \simeq (\mathscr{I}_k(f)/\mathscr{R}_{k,f}\cdot\mathscr{I}_k(f)^p) \,/\, (\mathscr{P}_k(f)\cdot\mathscr{I}_k(f)^p/\mathscr{R}_{k,f}\cdot\mathscr{I}_k(f)^p)$$

is equivalent to a direct product relation

$$\mathscr{I}_k(f)/\mathscr{R}_{k,f}\cdot\mathscr{I}_k(f)^p \simeq (\mathscr{I}_k(f)/\mathscr{P}_k(f)\cdot\mathscr{I}_k(f)^p) \times (\mathscr{P}_k(f)\cdot\mathscr{I}_k(f)^p/\mathscr{R}_{k,f}\cdot\mathscr{I}_k(f)^p),$$

where the first factor is isomorphic to the p-elementary class group of k. Further, the homomorphism $k^\times \to \mathscr{P}_k$, $\alpha \mapsto \alpha\mathscr{O}_k$ induces an isomorphism

$$\mathscr{P}_k(f)\cdot\mathscr{I}_k(f)^p/\mathscr{R}_{k,f}\cdot\mathscr{I}_k(f)^p \simeq k^\times(f)/(\mathbb{Q}^\times(f)\cdot k_f^\times\cdot I_{k,p}(f)).$$

Finally, it is well known that the local description of the congruence relation mod$^\times f$ yields an isomorphism

$$k^\times(f)/\mathbb{Q}^\times(f)\cdot k_f^\times \simeq (k^\times(f)/k_f^\times) \,/\, (\mathbb{Q}^\times(f)/\mathbb{Q}^\times(f)\cap k_f^\times) \simeq U(\mathscr{O}_k/f\mathscr{O}_k) \,/\, U(\mathbb{Z}/f\mathbb{Z})$$

and that the p-elementary subgroup of $U(\mathscr{O}_k/f\mathscr{O}_k)\,/\,U(\mathbb{Z}/f\mathbb{Z})$, which is isomorphic to $k^\times(f)/\mathbb{Q}^\times(f)\cdot k_f^\times\cdot k^\times(f)^p$, has p-rank equal $t+w$ [2, 6, 8], whence $\rho' = \rho + t + w - \delta$ with

$$\delta = \dim_{\mathbb{F}_p}(I_{k,p}(f)/I_{k,p}(f)\cap(\mathbb{Q}^\times(f)\cdot k_f^\times\cdot k^\times(f)^p)). \quad \square$$

Remarks. 1. For totally real dihedral fields, a further decomposition of the essential index p^δ into two parts is useful for practical purposes:

$$p^\delta = (I_{k,p}(f) : I_{k,p}(f)\cap(\mathbb{Q}^\times(f)k_f^\times U_k k^\times(f)^p))\cdot(U_k : U_k\cap(\mathbb{Q}^\times(f)k_f^\times k^\times(f)^p)),$$

where the first part involves only the principal pth powers of ideals which represent ρ generating classes of order p of k, and the second part concerns exclusively the fundamental unit of k. Here, U_k denotes the unit group of k.
2. The proof of Theorem 3.1 and the previous remark show that generally $\delta(f) \le \min(\rho, t+w)$ (in particular, $\delta(f) = 0$ when $\rho = 0$) in the cases $d_k < -3$ or $p \ge 5$, $d_k = -3$, and $\delta(f) \le \min(\rho+1, t+w)$ in the cases $d_k > 0$ or $p = 3$, $d_k = -3$.

Note. It should be pointed out that the proof of Theorem 3.1 does not use the full ray class group mod f of k but only the ring class group mod f of k, which is obtained from the former by factoring out the part invariant under the generating automorphism of $\mathrm{Gal}(k|\mathbb{Q})$ [6, 8]. Otherwise, there would be counted all cyclic extensions $N|k$ of degree p sharing the common conductor f, those with group $\mathrm{Gal}(N|\mathbb{Q}) \simeq D_p$ as well as those with group $\mathrm{Gal}(N|\mathbb{Q}) \simeq C(2)\times C(p)$ (composita of k with cyclic extensions $K|\mathbb{Q}$ of degree p).

The only case where the sum in the formula of Theorem 3.1 consists of a single term is the unramified case $f = 1$, which was treated in [8, p. 581] and [14] already.

Corollary 3.1. *The number of unramified cyclic extensions $N|k$ of degree p is*

$$m_p(d_k, 1) = \frac{1}{p-1}(p^\rho - 1).$$

Proof. If $f = 1$, that is, $t = 0$ and $w = 0$, then we have $\delta(f) = 0$, since $\delta(f) \leq \min(\rho + 1, t + w) = 0$, or also simply since $k_f^\times = k^\times$. □

In all other cases, single multiplicities can be obtained by Moebius inversion.

Theorem 3.2 (General multiplicity formula when $w \leq 1$). *Assume that $f = p^e \cdot q_1 \cdots q_t > 1$ with $w \leq 1$ is a p-admissible conductor for the quadratic field k, put $q_{t+1} = p^e$ when $w = 1$, and define $\delta_{\max} = \max\{\delta(q_{i_1} \cdots q_{i_s}) \mid 0 \leq s \leq t + w,\ 1 \leq i_1 < \cdots < i_s \leq t + w\}$. Then*

$$m_p(d_k, q_1 \cdots q_{t+w}) = p^\rho \cdot \frac{1}{p^{\delta_{\max}}} \cdot \left[(p-1)^{t+w-1} + \sum_{s=0}^{t+w} (-1)^{t+w-s} \cdot p^s \sum_{1 \leq i_1 < \cdots < i_s \leq t+w} \frac{p^{\delta_{\max} - \delta(q_{i_1} \cdots q_{i_s})} - 1}{p-1} \right].$$

Proof. Observe that, for fixed p and d_k, the general formula in Theorem 3.1,

$$\sum_{f'|f} m_p(d_k, f') = \frac{1}{p-1}(p^{\rho+t+w-\delta} - 1),$$

can be viewed as the sum relation $\sum_{f'|f} m(f') = n(f)$ between two integer-valued functions $n(f) = \frac{1}{p-1}(p^{\rho+t(f)+w(f)-\delta(f)} - 1)$ and $m(f') = m_p(d_k, f')$. Hence, an application of the Moebius inversion formula yields an expression for a single multiplicity,

$$\begin{aligned} m(q_1 \cdots q_{t+w}) &= \sum_{s=0}^{t+w} \sum_{1 \leq i_1 < \cdots < i_s \leq t+w} \mu\left(\frac{q_1 \cdots q_{t+w}}{q_{i_1} \cdots q_{i_s}}\right) \cdot n(q_{i_1} \cdots q_{i_s}) \\ &= \sum_{s=0}^{t+w} \sum_{1 \leq i_1 < \cdots < i_s \leq t+w} (-1)^{t+w-s} \cdot \frac{1}{p-1} \left(p^\rho \cdot p^s \cdot \frac{1}{p^{\delta(q_{i_1} \cdots q_{i_s})}} - 1 \right) \\ &= \sum_{s=0}^{t+w} \sum_{1 \leq i_1 < \cdots < i_s \leq t+w} (-1)^{t+w-s} \cdot \frac{1}{p-1} \cdot p^\rho \cdot p^s \cdot \frac{1}{p^{\delta(q_{i_1} \cdots q_{i_s})}} \\ &\quad - \frac{1}{p-1} \sum_{s=0}^{t+w} (-1)^{t+w-s} \sum_{1 \leq i_1 < \cdots < i_s \leq t+w} 1. \end{aligned}$$

Now the second double sum equals $\sum_{s=0}^{t+w}(-1)^{t+w-s}\cdot\binom{t+w}{s}=0$; hence,

$$m(q_1\cdots q_{t+w})=\frac{1}{p-1}\cdot p^{\rho}\cdot\frac{1}{p^{\delta_{\max}}}\cdot\left[\sum_{s=0}^{t+w}(-1)^{t+w-s}\cdot p^{s}\sum_{1\le i_1<\cdots<i_s\le t+w}1+\sum_{s=0}^{t+w}\sum_{1\le i_1<\cdots<i_s\le t+w}(-1)^{t+w-s}\cdot p^{s}\cdot(p^{\delta_{\max}-\delta(q_{i_1}\cdots q_{i_s})}-1)\right],$$

where the first double sum equals $\sum_{s=0}^{t+w}(-1)^{t+w-s}\cdot p^{s}\cdot\binom{t+w}{s}=(p-1)^{t+w}$; thus,

$$m(q_1\cdots q_{t+w})=\frac{1}{p-1}\cdot p^{\rho}\cdot\frac{1}{p^{\delta_{\max}}}\cdot\left[(p-1)^{t+w}+\sum_{s=0}^{t+w}\sum_{1\le i_1<\cdots<i_s\le t+w}(-1)^{t+w-s}\cdot p^{s}\cdot(p^{\delta_{\max}-\delta(q_{i_1}\cdots q_{i_s})}-1)\right].\quad\square$$

This formula can be simplified further, since the indices for composed conductors, $\delta(q_{i_1}\cdots q_{i_s})$ with $0\le s\le t+w$ and $1\le i_1<\cdots<i_s\le t+w$, can be determined from those for prime conductors, $\delta(q_i)$ with $1\le i\le t+w$.

Corollary 3.2 (The special cases of $\delta_{\max}=0,1$ when $w\le 1$). *Let* $f=p^{e}\cdot q_1\cdots q_t>1$ *with* $w\le 1$ *be a* p*-admissible conductor for the quadratic field* k, *put* $q_{t+1}=p^{e}$ *when* $w=1$, *suppose that* $\delta_{\max}<2$, *and put* $u=\#\{1\le i\le t+w\mid\delta(q_i)=0\}$, *i.e.,* $v:=t+w-u$ *is the number of "bad" primes.*

1 (The case without constraints from principal pth ideal powers [8, p. 582]). *If* $u=t+w$, *then* $\delta_{\max}=0$ *and*

$$m_p(d_k\,,\,q_1\cdots q_{t+w})=p^{\rho}\cdot(p-1)^{t+w-1}\,.$$

2 (Restrictions caused by principal pth ideal powers). *If* $0\le u\le t+w-1$, *then* $\delta_{\max}=1$ *and*

$$m_p(d_k\,,\,q_1\cdots q_{t+w})=p^{\rho}\cdot(p-1)^{u}\cdot\frac{(p-1)^{v-1}-(-1)^{v-1}}{p}\,.$$

In particular, $m_p(d_k\,,\,q_1\cdots q_{t+w})=0$ *for* $v=1$.

Proof. 1. If $u=t+w$, then $\delta(q_i)=0$ for all $1\le i\le t+w$, and consequently $\delta(q_{i_1}\cdots q_{i_s})=0$ for all $0\le s\le t+w$ and $1\le i_1<\cdots<i_s\le t+w$, whence $\delta_{\max}=0$. In this case, the formula of Theorem 3.2 immediately degenerates to

$$m_p(d_k\,,\,q_1\cdots q_{t+w})=p^{\rho}\cdot(p-1)^{t+w-1}\,.$$

2. If $0\le u\le t+w-1$, then $\delta(q_i)=1$ for some $1\le i\le t+w$, and thus $\delta_{\max}=1$. In this case, it turns out that

$$\#\{1\le i_1<\cdots<i_s\le t+w\mid\delta(q_{i_1}\cdots q_{i_s})=0\}=\binom{u}{s}$$

for all $0 \leq s \leq t+w$, whence

$$m_p(d_k, q_1 \cdots q_{t+w})$$

$$= p^\rho \cdot \frac{1}{p^{\delta_{\max}}} \cdot \left[(p-1)^{t+w-1} + \sum_{s=0}^{t+w} (-1)^{t+w-s} \cdot p^s \sum_{1 \leq i_1 < \cdots < i_s \leq t+w} \frac{p^{\delta_{\max} - \delta(q_{i_1} \cdots q_{i_s})} - 1}{p-1} \right]$$

$$= p^\rho \cdot \frac{1}{p} \cdot \left[(p-1)^{t+w-1} + \sum_{s=0}^{t+w} (-1)^{t+w-s} \cdot p^s \cdot \binom{u}{s} \cdot \frac{p-1}{p-1} \right]$$

$$= p^\rho \cdot \frac{1}{p} \cdot \left[(p-1)^{t+w-1} + (-1)^{t+w-u} \sum_{s=0}^{u} \binom{u}{s} \cdot (-1)^{u-s} \cdot p^s \right]$$

$$= p^\rho \cdot \frac{1}{p} \cdot [(p-1)^{t+w-1} + (-1)^{t+w-u}(p-1)^u]$$

$$= p^\rho \cdot (p-1)^u \cdot \frac{(p-1)^{t+w-1-u} + (-1)^{t+w-u}}{p} . \quad \square$$

The following array shows the multiplicities $m_p(d_k, q_1 \cdots q_{t+w})$ in dependence on the total number $t+w > 0$ of prime divisors of the conductor $f > 1$, and on the number $0 \leq u \leq t+w$ of those "nice" primes which do not cause restrictions, for the special case $p = 3$ and $\rho = 0$. For positive 3-rank $\rho > 0$ of k, the numbers must only be multiplied by 3^ρ, provided that still $\delta_{\max} < 2$.

$t+w$	$u=$	0	1	2	3	4	5	6	7	8
1		0	1							
2		1	0	2						
3		1	2	0	4					
4		3	2	4	0	8				
5		5	6	4	8	0	16			
6		11	10	12	8	16	0	32		
7		21	22	20	24	16	32	0	64	
8		43	42	44	40	48	32	64	0	128

Example 1. For pure cubic fields $L = \mathbb{Q}(\sqrt[3]{D})$, the formulas with $w = e \leq 1$ of Theorem 2.1 in the previous section, which were proved by elementary methods, can be reobtained here as the special case $p = 3$, $d_k = -3$, $\rho = 0$, and $u = \#\{1 \leq i \leq t+w \mid q_i \equiv \pm 1 \pmod 9\}$, since for any $1 \leq i \leq t+w$ the condition $\delta(q_i) = 0$ is equivalent to $\zeta_3 \in \mathbb{Q}^\times(q_i) \cdot k_{q_i}^\times \cdot k^\times(q_i)^3$ and hence to $q_i \equiv \pm 1 \pmod 9$:

$$m_3(-3, q_1 \cdots q_{t+w}) = 2^u \cdot \frac{2^{v+w-1} - (-1)^{v+w-1}}{3} ,$$

where $v := t-u$ and $v+w$ is the number of bad primes.

Finally, supplementary formulas must be established for the special case $p = 3$, $d_k \equiv -3 \pmod 9$, $w = 2$.

Theorem 3.3 (General multiplicity formula when $w = 2$). *Let $f = 3^2 \cdot q_1 \cdots q_t$ with $w = 2$ be a 3-admissible conductor for the quadratic field k. Then*

$$m_3(d_k, 3^2 \cdot q_1 \cdots q_t) = 3^\rho \sum_{s=0}^{t} (-1)^{t-s} \cdot 3^s \sum_{1 \le i_1 < \cdots < i_s \le t} \frac{1}{2}(3^{2-\delta(3^2 \cdot q_{i_1} \cdots q_{i_s})} - 3^{1-\delta(3 \cdot q_{i_1} \cdots q_{i_s})}) .$$

Proof. An application of the Moebius inversion formula to the sum relation $n(f) = \sum_{f'|f} m(f')$ in Theorem 1.1, where $n(f) = \frac{1}{2}(3^{\rho+t(f)+w(f)-\delta(f)} - 1)$ and $m(f') = m_3(d_k, f')$, yields an expression for the single multiplicity of the conductor $f = 3^2 \cdot q_1 \cdots q_t$:

$$m(3^2 \cdot q_1 \cdots q_t) = \sum_{v=0}^{2} \sum_{s=0}^{t} \sum_{1 \le i_1 < \cdots < i_s \le t} \mu\left(\frac{3^2 \cdot q_1 \cdots q_t}{3^v \cdot q_{i_1} \cdots q_{i_s}}\right) \cdot n(3^v \cdot q_{i_1} \cdots q_{i_s}) ,$$

where the Moebius function takes the values

$$\begin{cases} 0 & \text{if } v = 0, \\ (-1)^{t-s+1} & \text{if } v = 1, \\ (-1)^{t-s} & \text{if } v = 2. \end{cases}$$

Consequently,

$$\begin{aligned} m(3^2 \cdot q_1 \cdots q_t) &= \sum_{s=0}^{t} \sum_{1 \le i_1 < \cdots < i_s \le t} \left[(-1)^{t-s+1} \cdot \frac{1}{2}\left(3^\rho \cdot 3^{s+1} \cdot \frac{1}{3^{\delta(3 \cdot q_{i_1} \cdots q_{i_s})}} - 1\right)\right. \\ &\qquad \left. + (-1)^{t-s} \cdot \frac{1}{2}\left(3^\rho \cdot 3^{s+2} \cdot \frac{1}{3^{\delta(3^2 \cdot q_{i_1} \cdots q_{i_s})}} - 1\right)\right] \\ &= 3^\rho \sum_{s=0}^{t} (-1)^{t-s} \cdot 3^s \sum_{1 \le i_1 < \cdots < i_s \le t} \frac{1}{2}(3^{2-\delta(3^2 \cdot q_{i_1} \cdots q_{i_s})} - 3^{1-\delta(3 \cdot q_{i_1} \cdots q_{i_s})}) . \quad \square \end{aligned}$$

Corollary 3.3 (The special cases of $\delta_{\max} = 0, 1$ when $w = 2$). *Let $f = 3^2 \cdot q_1 \cdots q_t$ with $w = 2$ be a 3-admissible conductor for the quadratic field k. Further, redefine $\delta_{\max} = \max\{\delta(3^v \cdot q_{i_1} \cdots q_{i_s}) \mid 0 \le v \le 2,\ 0 \le s \le t,\ 1 \le i_1 < \cdots < i_s \le t\}$, suppose that $\delta_{\max} < 2$, and put $u = \#\{1 \le i \le t \mid \delta(q_i) = 0\}$. Then*

$$m_3(d_k, 3^2 \cdot q_1 \cdots q_t) = \begin{cases} 3^{\rho+1} \cdot 2^t & \text{if } \delta(3^2) = 0,\ u = t, \\ 3^{\rho+1} \cdot 2^{u+1} \cdot \frac{1}{3}(2^{t-u-1} - (-1)^{t-u-1}) & \text{if } \delta(3^2) = 0,\ 0 \le u \le t-1, \\ 3^{\rho+1} \cdot 2^u \cdot \frac{1}{3}(2^{t-u} - (-1)^{t-u}) & \text{if } \delta(3) = 0,\ \delta(3^2) = 1, \\ 3^\rho \cdot 2^t & \text{if } \delta(3) = 1. \end{cases}$$

The first case is the unconstrained one [8, *p.* 582] *where $\delta_{\max} = 0$, in the second case the multiplicity is zero for $u = t - 1$, in the third case for $u = t$, and the fourth case is actually independent of u.*

Proof. 1. If $\delta(3^2) = 0$, $u = t$, then clearly $\delta_{\max} = 0$, and the formula in Theorem 3.3 becomes

$$m_3(d_k, 3^2 \cdot q_1 \cdots q_t) = 3^\rho \sum_{s=0}^{t} (-1)^{t-s} \cdot 3^s \cdot \binom{t}{s} \cdot \frac{1}{2}(3^2 - 3) = 3^{\rho+1} \cdot 2^t .$$

2. However, if $\delta(3^2) = 0$ but $0 \le u \le t-1$, then certainly $\delta_{\max} = 1$, and $\delta(3^2 \cdot q_{i_1} \cdots q_{i_s}) = \delta(3 \cdot q_{i_1} \cdots q_{i_s}) = \delta(q_{i_1} \cdots q_{i_s})$ for all $0 \le s \le t$ and $1 \le i_1 < \cdots < i_s \le t$. In this case,

$$\begin{aligned} m_3(d_k, 3^2 \cdot q_1 \cdots q_t) &= 3^\rho \sum_{s=0}^{t} (-1)^{t-s} \cdot 3^s \sum_{1 \le i_1 < \cdots < i_s \le t} \frac{1}{2}(3^{2-\delta(q_{i_1} \cdots q_{i_s})} - 3^{1-\delta(q_{i_1} \cdots q_{i_s})}) \\ &= 3^\rho \sum_{s=0}^{t} (-1)^{t-s} \cdot 3^s \sum_{1 \le i_1 < \cdots < i_s \le t} \frac{1}{2}(3-1) \cdot 3^{1-\delta(q_{i_1} \cdots q_{i_s})} \\ &= 3^\rho \left[\sum_{s=0}^{t} (-1)^{t-s} \cdot 3^s \cdot \binom{t}{s} + (-1)^{t-u} \sum_{s=0}^{t} (-1)^{u-s} \cdot 3^s \cdot \binom{u}{s} \cdot (3-1) \right] \\ &= 3^\rho \cdot (2^t + (-1)^{t-u} \cdot 2^u \cdot 2) . \end{aligned}$$

3. In the case $\delta(3) = 0$, $\delta(3^2) = 1$, we have $\delta(3 \cdot q_{i_1} \cdots q_{i_s}) = \delta(q_{i_1} \cdots q_{i_s})$ and $\delta(3^2 \cdot q_{i_1} \cdots q_{i_s}) = 1$ for all $0 \le s \le t$ and $1 \le i_1 < \cdots < i_s \le t$, whence $\delta_{\max} = 1$ and

$$\begin{aligned} m_3(d_k, 3^2 \cdot q_1 \cdots q_t) &= 3^\rho \sum_{s=0}^{t} (-1)^{t-s} \cdot 3^s \sum_{1 \le i_1 < \cdots < i_s \le t} \frac{1}{2}(3 - 3^{1-\delta(q_{i_1} \cdots q_{i_s})}) \\ &= 3^\rho \sum_{s=0}^{t} (-1)^{t-s} \cdot 3^s \cdot \frac{1}{2}(3-1) \cdot \left[\binom{t}{s} - \binom{u}{s} \right] \\ &= 3^\rho \left[\sum_{s=0}^{t} (-1)^{t-s} \cdot 3^s \cdot \binom{t}{s} - (-1)^{t-u} \sum_{s=0}^{t} (-1)^{u-s} \cdot 3^s \cdot \binom{u}{s} \right] \\ &= 3^\rho \cdot (2^t - (-1)^{t-u} \cdot 2^u) . \end{aligned}$$

4. If, finally, $\delta(3) = 1$, then $\delta(3 \cdot q_{i_1} \cdots q_{i_s}) = 1$ and $\delta(3^2 \cdot q_{i_1} \cdots q_{i_s}) = 1$ for all $0 \le s \le t$ and $1 \le i_1 < \cdots < i_s \le t$, whence $\delta_{\max} = 1$ and

$$m_3(d_k, 3^2 \cdot q_1 \cdots q_t) = 3^\rho \sum_{s=0}^{t} (-1)^{t-s} \cdot 3^s \cdot \binom{t}{s} \cdot \frac{1}{2}(3-1) = 3^\rho \cdot 2^t . \quad \square$$

Example 2. For pure cubic fields $L = \mathbb{Q}(\sqrt[3]{D})$, the formula with $w = e = 2$ in Theorem 2.1 of the previous section can be reobtained as the special case $d_k = -3$, $\rho = 0$, and $\delta(3) = 1$:

$$m_3(-3, 3^2 \cdot q_1 \cdots q_t) = 2^t .$$

The various formulas of §3 are illustrated in the Supplements section at the end of this issue by a discussion of all known discriminants of multiplicity ≥ 5 of totally real and complex cubic fields, which occur in the most extensive recent numerical tables [10], [5].

Final Note. It should be particularly emphasized that all the calculations which are necessary for the determination of the multiplicity $m_p(d_k, f)$ of a dihedral discriminant $d_L = f^{p-1} d_k^{(p-1)/2}$ can be carried out entirely in the underlying quadratic field k.

Given a quadratic field k with p-class rank $\rho = \rho_k(p)$ and discriminant d_k, and given a p-admissible conductor f for d_k, we have to find ρ principal pth powers $\alpha_1, \ldots, \alpha_\rho$ of ideals prime to f which represent ρ generating classes of order p of the p-elementary class group of k, and additionally a fundamental unit η of k if $d_k > 0$ or $d_k = -3$. Then $I_{k,p}(f) = \langle \alpha_1, \ldots, \alpha_\rho(\ , \eta)\rangle \cdot k^\times(f)^p$.

Next, we must examine successively, if $\eta \in \mathbb{Q}^\times(f) \cdot k_f^\times \cdot k^\times(f)^p$ and if

$$\alpha_i \in \langle \alpha_1, \ldots, \alpha_{i-1}\rangle \cdot U_k \cdot \mathbb{Q}^\times(f) \cdot k_f^\times \cdot k^\times(f)^p \quad \text{for } i = 1, \ldots, \rho,$$

whence we will be able to determine $\delta(f')$ for all divisors $f'|f$ and finally the multiplicity $m_p(d_k, f)$ of $d_L = f^{p-1} d_k^{(p-1)/2}$, by means of Theorem 3.2 or 3.3.

In this manner it is possible to construct complete tables of complex or totally real dihedral discriminants up to a given bound, $|d_L| < B$, and for a fixed value of the prime p, by the computation of the p-ranks of ring class groups mod f of quadratic fields k, varying the discriminants d_k and the p-admissible conductors f for each discriminant d_k.

In particular, approximations can be determined for the asymptotic densities of dihedral discriminants for various primes $p \geq 5$, similar to the densities of Davenport and Heilbronn [3] for $p = 3$. As D. Shanks pointed out in his review [13] of [1], the convergence of these approximations to the asymptotic limits would be rather slow, because the really high multiplicities, which contribute the essential part to the limit, unfortunately occur in very high ranges of discriminants.

A drawback of the proposed method is that it does not seem to be suitable for obtaining generating polynomials for the non-Galois subfields L of dihedral fields.

Example. For any two positive integers m and B, let $n_p(m, B)$ denote the number of complex dihedral discriminants $d_L = f^{p-1} d_k^{(p-1)/2}$ of multiplicity $m_p(d_k, f) = m$, which are bounded by $|d_L| < B^{(p-1)/2}$. (Observe that dihedral discriminants are always complete $((p-1)/2)$th powers.)

To make the ideas in the final note more concrete, we have computed the 303 968 quadratic discriminants in the range $-10^6 < d_k < 0$ and determined the class numbers and p-class ranks $\rho = \rho_k(p)$ of the corresponding imaginary quadratic fields k for $p = 3, 5, 7$. With the aid of this information, we can calculate the exact numbers $n_p(m, B)$ for $m = 1, p-1, p+1$, and for any given upper bound $B \leq 10^6$.

(a) According to Corollary 3.1, the first component of $n_p(1, B)$ is the number of quadratic fields k with p-rank $\rho = 1$ and discriminant

$$|d_k| = |d_L|^{2/(p-1)} < B,$$

i.e., single unramified cyclic extensions (absolute class fields) $N|k$ of degree p with conductor $f = 1$.

By Corollary 3.2,1, the second component is the number of ramified cyclic extensions (ring class fields) N of degree p over quadratic fields k with p-rank $\rho = 0$ (and thus $\delta = 0$) and discriminant

$$|d_k| = |d_L / f^{p-1}|^{2/(p-1)} = |d_L|^{2/(p-1)} / f^2 < B / f^2$$

with a single prime divisor q_1 of the conductor f, such that $t + w = 1$. To compute this number, we examine each of the relevant quadratic discriminants d_k for admissible prime conductors $q_1 \equiv \pm 1 \pmod{p}$, also taking into consideration the possibility of $p|f$, $w = 1$.

In the case of $p = 3$, we must further add the number of pure cubic discriminants ($d_k = -3$) of multiplicity 1, which can be evaluated by counting primes and products of up to three primes below certain bounds, according to Theorem 2.1, taking into account the parameter values

$$(e, t) = (2, 0) \quad \text{and}$$
$$(e, u, v) = (1, 0, 1), (1, 0, 2), (0, 1, 0), (0, 0, 2), (0, 0, 3).$$

p	$(p-1)/2$	B	$n_p(1, B)$		$f = 1$		$f > 1$		
							$d_k < -3$		$d_k = -3$
3	1	10^3	125	=	84	+	35	+	6
		10^4	1 396	=	1 034	+	343	+	19
		10^5	14 565	=	11 286	+	3 215	+	64
		10^6	149 204	=	118 455	+	30 559	+	190
5	2	10^3	58	=	52	+		6	
		10^4	665	=	617	+		48	
		10^5	7 099	=	6 686	+		413	
		10^6	73 252	=	69 365	+		3 887	
7	3	10^3	31	=	30	+		1	
		10^4	435	=	411	+		24	
		10^5	4 709	=	4 503	+		206	
		10^6	49 607	=	47 595	+		2 012	

The result $n_3(1, 10^6) = 149\,204$, in comparison to the number 148 709 claimed in [5, Table 5.2, p. 321], shows that 495 complex cubic discriminants of multiplicity 1 were missing from the original version of [5].

The series of single complex dihedral discriminants starts with -23 for $p = 3$, with $+2209 = (-47)^2$ for $p = 5$, and with $-357\,911 = (-71)^3$ for $p = 7$. The minimal discriminants of arbitrary quintic fields with signature $(1, 2)$, resp. septic fields with signature $(1, 3)$, are somewhat smaller and not $((p-1)/2)$th powers: $+1\,609$, resp. $-184\,607$. Unramified extensions are dominating, 79.5% for $p = 3$, 94.7% for $p = 5$, and 95.9% for $p = 7$, and this effect even seems to increase with the value of the prime p. The minimal examples of the rare ramified extensions are $d_k = -11$ with $f = 2$ for $p = 3$, $d_k = -15$ with $f = 5$ for $p = 5$, and $d_k = -7$ with $f = 7$ for $p = 7$.

(b) By Corollary 3.2,1, $n_p(p-1, B)$ is the number of $(p-1)$-tuplets of ramified cyclic extensions N of degree p over quadratic fields k of p-rank $\rho = 0$ and discriminant $|d_k| < B/f^2$ with two prime divisors q_1, q_2 of the conductor f, such that $w \leq 1$.

But for the special case $p = 3$, the number of pure cubic discriminants of multiplicity 2 must be added. According to Theorem 2.1, we determine this number by counting primes and products of at most four primes up to certain

bounds, taking into consideration the parameter values

$$(e, t) = (2, 1) \quad \text{and}$$
$$(e, u, v) = (1, 1, 1), (1, 1, 2), (0, 2, 0), (0, 1, 2), (0, 1, 3).$$

It might be of interest to list explicitly the root discriminants $|d_L|^{2/(p-1)}$ for the few encountered $(p-1)$-tuplets of dihedral fields with two prime divisors of the conductor f, if $p = 5, 7$ (for $p = 3$, they start with the well-known 1836 [1]).

There are 20 cases for $p = 5$:

105 875, 121 000, 180 500, 287 375, 305 767, 315 375, 315 875, 360 375, 363 000, 496 375, 529 375, 589 875, 605 000, 650 375, 771 375, 786 500, 814 088, 840 500, 841 000, 902 500,

and 7 cases for $p = 7$:

57 967, 288 463, 576 583, 634 207, 695 604, 985 439, 994 903.

p	$(p-1)/2$	B	$n_p(p-1, B)$		$f > 1$		
					$d_k < -3$		$d_k = -3$
3	1	10^3	1	=	0	+	1
		10^4	12	=	10	+	2
		10^5	167	=	157	+	10
		10^6	1 683	=	1 639	+	44
5	2	10^6	20	=		20	
7	3	10^5	1	=		1	
		10^6	7	=		7	

Here, the authors of [5] announce the value $n_3(2, 10^6) = 1\,762$ instead of 1 683. In fact, the multiplicities of the superfluous 79 discriminants must necessarily be greater than 2.

(c) The determination of $n_p(p, B)$ is much more difficult, since it involves the complete treatment of various cases of p-tuplets of ramified cyclic extensions N of degree p over quadratic fields k of p-rank $\rho \geq 1$ and discriminant $|d_k| < B/f^2$ with conductor $f > 1$, according to Corollary 3.2. If $p = 3$, then further contributions arise from Corollary 3.3. Here, $\delta \geq 1$ is possible, and thus the principal pth powers $\alpha_1, \ldots, \alpha_\rho$ of ideals of k must be examined for each of the relevant quadratic discriminants d_k.

(d) By Corollary 3.1, $n_p(p+1, B)$ is the number of quadratic fields k with p-rank $\rho = 2$ and discriminant $|d_k| < B$, i.e., $(p+1)$-tuplets of unramified cyclic extensions $N|k$ of degree p with conductor $f = 1$.

In the case of $p = 3$, where exceptionally not only $(p^2-1)/(p-1) = p+1$ but also $(p-1)^2 = p+1$, we must additionally consider the number of ramified cyclic extensions N of degree p over quadratic fields k of p-rank $\rho = 0$ and discriminant $|d_k| < B/f^2$ with three prime divisors q_1, q_2, q_3 of the conductor f, such that $w \leq 1$.

A further additive component for $p = 3$ is the number of pure cubic discriminants of multiplicity 4, which can again be evaluated with the aid of Theorem 2.1 by counting products of up to five primes below certain bounds, taking into

account the parameter values

$$(e, t) = (2, 2) \text{ and}$$
$$(e, u, v) = (1, 2, 1), (1, 2, 2), (0, 3, 0), (0, 2, 2), (0, 2, 3).$$

p	$(p-1)/2$	B	$n_p(p+1, B)$		$f=1$		$f>1$		
							$d_k < -3$		$d_k = -3$
3	1	10^4	7	=	7	+	0	+	0
		10^5	216	=	214	+	0	+	2
		10^6	3216	=	3190	+	15	+	11
5	2	10^5	39	=	39				
		10^6	398	=	398				
7	3	10^5	1	=	1				
		10^6	97	=	97				

The result $n_3(4, 10^6) = 3216$, in comparison to the number 3189 given in [5], reveals the lack of 27 complex cubic discriminants of multiplicity 4 in the original version of [5].

(e) Finally it should be mentioned, that the authors of [5] announced the extremely exciting number $n_3(5, 10^6) = 7$, which caused a lot of confusion. However, our Example 5 after Theorem 2.1 shows that the minimal occurrence $d_L = -16\,008\,300$ of multiplicity 5 (which is only possible for pure and certain totally real cubic fields) lies considerably outside the range of the computations in [5].

Bibliography

1. I. O. Angell, *A table of complex cubic fields*, Bull. London Math. Soc. **5** (1973), 37–38.
2. T. Callahan, *Dihedral field extensions of order* $2p$ *whose class numbers are multiples of* p, Canad. J. Math. **28** (1976), 429–439.
3. H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields.* II, Proc. Roy. Soc. London Ser. A **322** (1971), 405–420.
4. R. Dedekind, *Über die Anzahl der Idealklassen in reinen kubischen Zahlkörpern*, J. Reine Angew. Math. **121** (1900), 40–123.
5. G. W. Fung and H. C. Williams, *On the computation of a table of complex cubic fields with discriminant* $D > -10^6$, Math. Comp. **55** (1990), 313–325.
6. F. Gerth III, *Cubic fields whose class numbers are not divisible by* 3, Illinois J. Math. **20** (1976), 486–493.
7. M. N. Gras, *Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de* $\mathbb{Q}$, J. Reine Angew. Math. **277** (1975), 89–116.
8. H. Hasse, *Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage*, Math. Z. **31** (1930), 565–582.
9. ———, *Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern*, Abh. Deutsche Akad. Wiss. Berlin **2** (1950), 3–95.
10. P. Llorente and J. Quer, *On totally real cubic fields with discriminant* $D < 10^7$, Math. Comp. **50** (1988), 581–594.
11. D. C. Mayer, *Table of pure cubic number fields with normalized radicands between* 0 *and* 100 000, Univ. Graz, 1989.
12. ———, *Table of simply real cubic number fields with discriminants between* $-30\,000$ *and* 0, Univ. Graz, 1989.

13. D. Shanks, Review of I. O. Angell, *Table of complex cubic fields*, Math. Comp. **29** (1975), 661–665.

14. O. Taussky, *A remark concerning Hilbert's Theorem 94*, J. Reine Angew. Math. **239/240** (1970), 435–438.

15. B. M. Urazbaev, *The distribution of the discriminants of cyclic fields of prime degree*, Izv. Akad. Nauk Kazakh. SSR, Ser. Fiz.-Mat., **1** (1969), 8–14. (Russian)

Department of Computer Science, University of Manitoba, Winnipeg, Manitoba, Canada R3T 2N2

E-mail address: mayer@gold.cs.umanitoba.ca