

ACTA ARITHMETICA XLIX (1987)

New formulas for the class number of imaginary quadratic fields

by

MARTIN EICHLER (Basel)

Dedicated to Paul Erdős at his 75th birthday

Introduction. Fifty years ago the result of this paper may have met with more interest than today. But at that time began the mathematical career of Paul Erdős. Therefore I dedicate my paper to the mathematician who knew how to proceed from easy standpoints to deep discoveries.

Let q be one of the primes 2, 3, 5, 7, 13 and K(q) the quaternion algebra over Q which is only ramified at the places ∞ and q. In these algebras all maximal orders are isomorphic. We fix one of them: $\Im(q)$. The number of left $\Im(q)$ -ideals is 1.

We consider the imaginary quadratic fields $Q(\sqrt{-d})$ which can be imbedded in K(q). The element $\omega = \sqrt{-d}$ can be imbedded in $\Im(q)$ if $d \not\equiv 7 \mod 8$ for q = 2 and if the Legendre symbol $\left(\frac{-d}{q}\right) \not\equiv 1$ for q > 2. The number of imbeddings of ω in $\Im(q)$ is, up to an elementary factor, equal to the ideal class number h of $Q(\omega)$.

In this paper we will study the number of pairs $(\omega_1, \omega_2) \in \mathfrak{I}(q)$ with $\omega_1^2 = \omega_2^2 = -d$. Their number is roughly equal to the square of the ideal class number.

On the other hand, the number of these pairs can be explicitly determined in the following way (for the sake of simplicity we assume $d \not\equiv 3 \mod 4$, then the order $v = [1, \omega]$ is maximal). To a pair (ω_1, ω_2) we attach the order

$$\mathfrak{D}(s) = (1, \, \omega_1, \, \omega_2, \, \frac{1}{2}(s + \omega_1 \, \omega_2 - \omega_2 \, \omega_1))$$

with $s = s(\omega_1 \omega_2)$, the trace. It is abstractly determined by d and s. Let E(q, d, s) be the number of different maximal orders with discriminant q^2 which contain $\mathfrak{D}(s)$. Then

$$\sum_{s} E(q, d, s)$$

equals the number of pairs $(\omega_1, \omega_2) \in \Im(q)$ up to an elementary factor. See Theorem 1. This number will be explicitly determined in Theorem 2 and its corollary.

Two features of our formulas are remarkable. Firstly they give formally different expressions for h in case $Q(\omega)$ can be imbedded in more than one K(q). Secondly they resemble Dirichlet's class number formula. This formula has even been proved by B. A. Wenkov: Ueber die Klassenzahl positiver binärer quadratischer Formen (Math. Zeitschr. 33 (1931), pp. 350-374), using ideas which are not far from ours. Wenkov starts from a formula given by Gauss in his Disquisitiones Arithmeticae, for the number of expressions of a given quadratic form as the sum of three squares of linear forms:

$$ax^2 + 2bxy + cy^2 = \sum_{v=1}^{3} (u_v x + v_v y)^2 = n(\eta_1 x + \eta_2 y)$$

or, in our language, as the reduced norm from K(2) where η_1 , η_2 have traces 0. This number is equal to the number of maximal orders in K(2) which contain the abstract order

$$\mathfrak{D} = (1, \eta_1, \eta_2, \frac{1}{2}(s(\eta_1 \eta_2) + \eta_1 \eta_2 - \eta_2 \eta_1)).$$

The knowledge of this number leads by elementary but rather lengthy considerations to Dirichlet's class number formula in the case $d \not\equiv 7 \mod 8$.

Assumptions and notation.

d > 3 is a square-free natural integer;

$$\alpha = \begin{cases} \omega = \sqrt{-d} & \text{for } d \equiv 1, 2 \mod 4, \\ \frac{1}{2}(1+\omega) & \text{for } d \equiv 3 \mod 4; \end{cases}$$

 ω_1 , ω_2 and α_1 , α_2 are imbeddings of ω and α in $\Im(q)$. They exist if

$$d \not\equiv 7 \mod 8$$
 for $q = 2$,

$$\left(\frac{-d}{q}\right) \neq 1$$
 for $q > 2$;

 $\Delta = -4d$ resp. -d is the discriminant of $Q(\omega)$; h is the ideal class number of $Q(\omega)$;

$$r(q, d) = \begin{cases} 2 & \text{if } q \text{ is ramified in } Q(\omega), \\ 1 & \text{otherwise:} \end{cases}$$

N(q) = 24, 12, 6, 4, 2 for q = 2, 3, 5, 7, 13 is the number of isomorphisms

$$\mathfrak{I}(q) \to \eta^{-1} \, \mathfrak{I}(q) \, \eta;$$

$$D = \begin{cases} 4(4d^2 - s^2)^2 & \text{for } d \equiv 1 \text{ or } 2 \mod 4, \\ \frac{1}{4}(d^2 - s_1^2)^2 & \text{for } d \equiv 3 \mod 4 \end{cases}$$

is the discriminant of $\mathfrak{D}(s)$, see Proposition 1, where

$$s = s(\omega_1 \omega_2), \quad s_1 = \frac{1}{2}s.$$

1. The order $\mathfrak{D}(s)$.

Proposition 1A. Let $d \not\equiv 3 \mod 4$. Then an order

$$\mathfrak{D}(s) = (1, \, \omega_1, \, \omega_2, \, \frac{1}{2}(s+\Omega))$$

in a quaternion algebra is defined by the relations

(1)
$$\omega_1^2 = \omega_2^2 = -d, \quad s = \omega_1 \omega_2 + \omega_2 \omega_1,$$

(2)
$$\Omega = \omega_1 \, \omega_2 - \omega_2 \, \omega_1, \quad \omega_i \, \Omega + \Omega \omega_i = 0.$$

$$\Omega^2 = s^2 - 4d^2$$

Its discriminant is

$$D = 4(4d^2 - s^2)^2$$

Remark. If q = 2, s is even.

Proof. From (1), (2) it follows that

$$s^2 = (\omega_1 \, \omega_2)^2 + (\omega_2 \, \omega_1)^2 + 2d$$

$$\Omega^2 = (\omega_1 \, \omega_2)^2 + (\omega_2 \, \omega_1)^2 - 2d$$

and hence (3). Furthermore

$$\omega_1 \, \omega_2 = \frac{1}{2} (s + \Omega).$$

$$\omega_1 \Omega = -2d\omega_2 - s\omega_1,$$

$$\omega_1 \frac{1}{2} (s + \Omega) = -d\omega_2$$
, $\omega_2 \frac{1}{2} (s + \Omega) = d\omega_1 + s\omega_2$.

The other products of the basis elements follow from these.

Proposition 1B. Let $d \equiv 3 \mod 4$. In this case we define

$$\mathfrak{D}(s) = (1, \alpha_1, \alpha_2, \alpha_1 \alpha_2)$$

with the same relations (1)–(3) where $\alpha_i = \frac{1}{2}(1+\omega_i)$. The discriminant is

$$D = \frac{1}{4}(d^2 - s_1^2)^2, \quad s_1 = \frac{1}{2}s.$$

Proof. Now we have

$$\alpha_1 \alpha_2 = \frac{1}{4} (1 + \omega_1 + \omega_2 + s_1 + \frac{1}{2} \Omega) = \frac{1}{4} (\alpha_1 + \alpha_2) + \frac{1}{4} (s_1 - 1) + \frac{1}{6} \Omega$$

and

$$\begin{split} \alpha_2 \frac{1}{4} \Omega &= \frac{1}{8} \Omega + \frac{1}{4} (d\omega_1 + s\omega_2) \\ &= \frac{1}{8} \Omega + \frac{1}{2} (\alpha_1 + \alpha_2) + \frac{1}{2} (d-1) \alpha_1 + \frac{1}{2} (s_1 - 1) \alpha_2 + \frac{1}{4} (d+s_1) \\ &= \alpha_1 \alpha_2 + \frac{1}{2} (d-1) \alpha_1 + \frac{1}{2} (s_1 - 1) \alpha_2 + \frac{1}{4} (d+1) - \frac{1}{2} (d+s_1). \end{split}$$

All other products of the basis elements can be got from these.

Our chief task is the determination of the number E(q, d, s) of maximal orders containing $\mathfrak{D}(s)$ which are isomorphic to $\mathfrak{I}(q)$. Evidently this number is the product of its local contributions

(4)
$$E(q, d, s) = \prod_{p} E(q, d, s)_{p}.$$

We begin with considering the latter.

Proposition 2. The number of maximal orders containing the p-adic extension $\mathfrak{D}(s)_p$ which are isomorphic to $\mathfrak{I}(q)_p$ is

$$E(q, d, s)_p = 1$$
 if $p \nmid D$.

Now, assume p does not divide the discriminant Δ of $\mathbf{Q}(\omega)$. Then

$$E(2, d, s)_2 = \begin{cases} 0 & \text{if } d \equiv 7 \mod 8, \\ 1 & \text{otherwise} \end{cases}$$

and for q > 2

$$E(q, d, s)_q = \begin{cases} 0 & \text{if} \quad q \text{ does not divide } D, \\ \sum \left(\frac{\Delta}{t_q}\right) & \text{with the Legendre symbol,} \end{cases}$$

with the sum extended over all q-adic divisors t_q of $q^{-1}D$. Finally, for a prime $p \neq q$ which does not divide both D and Δ ,

$$E(q, d, s)_p = \sum_{p} \left(\frac{\Delta}{t_p}\right)$$
 with the Legendre symbol,

with the sum extended over all p-adic divisors t_p of D.

Proof. First let us consider the case p = q. The statement for q = 2 is known. For q > 2 it means that $E(q, d, s)_q$ is 0 or 1 according as D is divisible by q an even or odd number of times. This is also evident.

Now let $p \neq q$, $p \neq 2$ and $p \not\vdash \Delta$. A basis of $\mathfrak{D}(s)_p$ is

(5)
$$1, \omega_1, \omega_2', \Omega \quad \text{with} \quad \omega_2' = \frac{s}{2d}\omega_1 + \omega_2$$

where

$$\omega_1 \, \omega_2' + \omega_2' \, \omega_2 = 0, \quad \omega_2'^2 = (4d)^{-1} \, (s^2 - 4d^2), \quad \omega_1 \, \omega_2' = \frac{1}{2} \Omega.$$

It can be represented by the matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} r & 0 \\ 0 & -r \end{bmatrix}, \quad \begin{bmatrix} 0 & m \\ p^{\alpha} & 0 \end{bmatrix}, \quad \begin{bmatrix} r & 0 \\ 0 & -r \end{bmatrix} \begin{bmatrix} 0 & m \\ p^{\alpha} & 0 \end{bmatrix}$$

where $r^2 = -d$, $m \not\equiv 0 \mod p$ and p^{α} is the greatest power of p dividing D. This

order is contained in the maximal orders

$$\begin{bmatrix} 0 & mp^{v-\alpha} \\ p^{\alpha-v} & 0 \end{bmatrix}, \quad 0 \le v \le \alpha$$

and in no others. And α can be written as the sum over the divisors $p^{\nu} = t_p$. For p = 2 which still does not divide Δ , a basis of $\mathfrak{D}(s)_2$ can be taken from Proposition 1B (with $s_1 = \frac{1}{2}s$)

1,
$$\frac{1}{2}(1+\omega_1)$$
, $\frac{1}{2}\left(\frac{s_1}{d}\omega_1+\omega_2\right)$, $\frac{1}{2}(1+\omega_1)\frac{1}{2}\left(\frac{s_1}{d}\omega_1+\omega_2\right)$.

It can be represented by the matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \frac{1}{2} \begin{bmatrix} 1+r & 0 \\ 0 & 1-r \end{bmatrix}, \quad \begin{bmatrix} 0 & m \\ 2^{x} & 0 \end{bmatrix}, \quad \frac{1}{2} \begin{bmatrix} 1+r & 0 \\ 0 & 1-r \end{bmatrix} \begin{bmatrix} 0 & m \\ 2^{x} & 0 \end{bmatrix}$$

where 2^{α} is the greatest power of 2 dividing $\frac{1}{4}(s_1^2 - d^2)$. The number of maximal orders containing $\mathfrak{D}(s)_2$ is the same as in the case p > 2.

Proposition 3. For an odd p dividing D and Δ

$$E(q, d, s)_p = 1 + \left(\frac{d^{-1}(s_1^2 - d^2)p^{-2v}}{p}\right) + \left(\frac{(s_1^2 - d^2)p^{-2v'}}{p}\right)$$

where p^{2v} and $p^{2v'}$ are the greatest even powers of p dividing $d^{-1}(s_1^2-d^2)$ and $(s_1^2-d^2)$ respectively. One of these symbols is 0, the other +1.

Proof. By assumption, $s \equiv 0 \mod p$. We use the basis (5) of $\mathfrak{D}(s)_p$. Let

$$\eta = p^{-1}(a_1 \omega_1 + a_2 \omega_2' + a_3 \Omega)$$

lie in a proper extension of $\mathfrak{D}(s)_p$. Then

$$\eta^2 = p^{-2} \left(-da_1^2 + (s^2 - 4d^2)(4d)^{-1} a_2^2 + (s^2 - 4d^2) 4^{-1} a_3^2 \right) \in \mathbb{Z}_p.$$

If the coefficients of a_2^2 and a_3^2 are both divisible by p^2 , a_1 must be $\equiv 0 \mod p$, and then we may assume $a_1 = 0$. Then every extension of $\mathfrak{D}(s)_p$ contains

$$\mathfrak{D}'_{p} = (1, \omega_{1}, p^{-1}\omega'_{2}, p^{-1}\Omega).$$

The same procedure may be repeated until we arrive at

$$\mathfrak{D}_p^{\prime\prime} = (1, \, \omega_1, \, p^{-\nu} \omega_2^{\prime}, \, p^{-\nu} \Omega)$$

where now $(s^2 - 4d^2)(4dp^{2\nu})^{-1}$ is no longer divisible by p^2 . If it is divisible by p, every larger order containing \mathfrak{D}_p'' lies in

$$\mathfrak{D}_{n}^{m} = (1, \omega_{1}, p^{-\nu}\omega_{2}^{\nu}, p^{-\nu-1}\Omega)$$

and $(s^2-4d^2)(4dp^{2\nu+2})^{-1} \not\equiv 0 \bmod p$.

We must distinguish 2 cases:

1. $(s^2-4d^2)(4dp^{2v})^{-1} \not\equiv 0 \bmod p$, but $(s^2-4d^2)(4p^{2v})^{-1} \equiv 0 \bmod p$. The quaternion algebra generated by \mathfrak{D}_p'' is ramified at p if $-(s^2-4d^2)(4dp^{2v})^{-1}$ is a quadratic non-residue mod p, and then $E(q, d, s)_p = 0$. Otherwise it is unramified, and then the argument in the proof of Proposition 2 shows that \mathfrak{D}_p'' is contained in 2 maximal orders. This is one case of contention.

2. $(s^2 - 4d^2)(4dp^{2\nu})^{-1} \equiv 0 \mod p$. Then $(s^2 - 4d^2)(4p^{2\nu+2})^{-1} \not\equiv 0 \mod p$, and we can reason as in case 1.

The determination of $E(q, d, s)_2$ for q > 2 is more complicated. For the sake of brevity we only remark

COROLLARY. If $E(q, d, s)_p \neq 0$ for all odd p, then $E(q, d, s)_2 \neq 0$.

Indeed, the assumption means that the algebra generated by $\mathfrak{D}(s)$ is ramified at ∞ and q and at no other odd p. Therefore it cannot be ramified at 2.

2. The number of pairs (ω_1, ω_2) . It is evident that there are as many pairs (ω_1, ω_2) as pairs (α_1, α_2) . Therefore we will only speak of the former. We refer to the notation explained in the introduction. The following is known:

Proposition 4. Under the assumption that $Q(\omega)$ can be imbedded in K(q), the number of ω or α in $\Im(q)$ is

$$N(q) h'$$
 with $h' = r(q, d)^{-1} h$.

Among all "equivalent" elements $\eta^{-1}\omega\eta$ with $\eta^{-1}\Im(q)\eta=\Im(q)$ we fix one and call it *normed*. A pair (ω_1, ω_2) will be called *normed* if ω_1 is normed.

The number of all pairs (ω_1, ω_2) is $N(q)^2 h'^2$. Among these there are 2N(q)h' "improper" pairs (ω, ω) resp. $(\omega, -\omega)$ to which there does not correspond an order $\mathfrak{D}(s)$ of rank 4. Consequently we have

$$N(q) h'^2 - 2h'$$

normed proper pairs.

We can count these pairs in yet another way. An order $\mathfrak{D}(s)$ is determined uniquely (up to isomorphism) by q, d, s and the relations in Proposition 1. $\mathfrak{D}(s)$ is contained in E(q, d, s) maximal orders \mathfrak{I}_i (i = 1, ..., E). Then for certain elements ϱ_i : $\mathfrak{I}(q) = \varrho_i^{-1} \mathfrak{I}_i \varrho_i$, and the pairs $(\omega_{i1}, \omega_{i2}) = \varrho_i^{-1} (\omega_1, \omega_2) \varrho_i$ lie in $\mathfrak{I}(q)$. For each of them there exists exactly one η with $\eta^{-1} \mathfrak{I}(q) \eta = \mathfrak{I}(q)$ such that $\eta^{-1} (\omega_{i1}, \omega_{i2}) \eta$ is normed. Therefore there exist E(q, d, s) normed pairs in $\mathfrak{I}(q)$ with given s, and we have proved

THEOREM 1. With the notation explained above and $h' = r(q, d)^{-1}h$ the class number h satisfies the equation

$$N(q) h'^2 - 2h' = \sum E(q, d, s)$$

with the sum extended over $-2d+1 \le s \le 2d-1$ in the case of $d \equiv 1$ or $2 \mod 4$ and $-d+1 \le s \le d-1$ for $d \equiv 3 \mod 4$.

It is easy to check the theorem numerically in the case q=2 and small d, since $E(q, d, s)_2 = 1$. Other easy cases are q > 2 and small $d \equiv 3 \mod 4$. Then we have again $E(q, d, s)_2 = 2$.

Now we transform the right-hand side, using (4) and the p-adic contributions $E(q, d, s)_p$ given in Section 1. We decompose the sum in Theorem 1:

(6)
$$E(q, d, d) = \sum_{T} E_{T}, \quad E_{T} = \sum_{s} E(q, d, s)$$

summed over all maximal common divisors $T = (\Delta, D)$.

 E_1 is easy, namely from Proposition 2 it follows that

(7)
$$E_{1} = \sum \left(\frac{\Delta}{t_{1} t_{2}}\right) \begin{cases} A(t_{1}, t_{2}, n) & \text{for } q = 2, \\ A(qt_{1}, t_{2}, n) & \text{for } q > 2, \end{cases}$$

where $A(t_1, t_2, n)$ means the number of positive integral solutions of

$$(8) t_1 x_1 + t_2 x_2 = n$$

and

(9)
$$n = \begin{cases} 4d & \text{for } d \equiv 1 \text{ or } 2 \mod 4, \\ 2d & \text{for } d \equiv 3 \mod 4. \end{cases}$$

The sum in (7) is extended over all positive relatively prime t_1 , t_2 which are both odd in the case q = 2, and satisfy $t_2 \not\equiv 0 \mod q$ for q > 2.

Proof of (7).

$$E(q, d, s) = \prod_{p} E(q, d, s)_{p} = \sum_{t} \left(\frac{\Delta}{t}\right),$$

with t running over all divisors of $4d^2-s^2$ resp. d^2-s^2 . These t are decomposed into $t=t_1\,t_2$ with t_1 dividing 2d-s resp. d-s and t_2 dividing 2d+s resp. d+s. t_1 and t_2 cannot have a common divisor >1 since it would divide Δ and Δ . In the case q>2 we have written qt_1 instead of t_1 .

We claim that

(10)
$$A(t_1, t_2, n) = \left[\frac{n}{t_1 t_2}\right].$$

Proof. We begin with a solution of (8) with $x_1 > 0$, $x_2 < 0$ and form a new solution $x_1' = x_1 - t_2$, $x_2' = x_2 + t_1$. We repeat this until $x_1^0 > 0$, $x_2^0 < 0$ is the last of this kind. Now we form the next solution

$$x_1^1 = x_1^0 - t_2, \quad x_2^1 = x_2^0 + t_1.$$

We have either $x_1^1 < 0$, $x_2^1 > 0$ or $x_1^1 > 0$, $x_2^1 > 0$ $(x_1^1 > 0, x_2^1 < 0 \text{ holds})$ no longer because of the assumption). In the first case (8) has no solution with $x_1 > 0$, $x_2 > 0$. Furthermore then

$$n = x_1^0 t_1 + x_2^0 t_2 < t_1 t_2$$
 or $n(t_1 t_2)^{-1} < 1$.

In the second case x_1^1 , x_2^1 is a solution, and we can construct further ones with a = 1, 2, ...

$$x_1^a = x_1^0 - at_2, \quad x_2^a = x_2^0 + at_1.$$

If this is done the last solution we have $x_1^0 < (a+1)t_2$ and

$$n = x_1^0 t_1 + x_2^0 t_2 < (a+1)t_1 t_2$$
 or $n(t_1 t_2)^{-1} < a+1$

and $a = [n/(t_1 t_2)].$

The other summands in (6) can at least be estimated:

(11)
$$0 \leqslant E_T \leqslant \sum_{t_1, t_2} \left(\frac{\Delta}{t_1 t_2} \right) \left[\frac{nT^{-1}}{(q)t_1 t_2} \right] 2^{\mathfrak{r}},$$

 τ = number of different primes dividing T, with n as in (8) and (q) = 1 or (q) = q according as q = 2 or q > 2.

We collect the results of (6) to (10):

THEOREM 2. The class number of the field $Q(\sqrt{-d})$ imbedded in K(q) satisfies the following equation:

(12)
$$N(q) h'^{2} - 2h' = \sum_{n} \left(\frac{\Delta}{t_{1} t_{2}}\right) \left[\frac{n}{(q) t_{1} t_{2}}\right] + \sum_{n} E_{n}$$

where n is given by (9) and (q) = 1 for q = 2 and (q) = q for q > 2. The sum is extended over all natural and relatively prime t_1 , t_2 where $(q, t_2) = 1$ in the case q > 2 and t_1 , t_2 are both odd in the case q = 2.

In the second sum T runs over all maximal common divisors of Δ and D which are > 1. The summands E_T can be estimated as in (11).

COROLLARY. If d is a prime and $\equiv 3 \mod 4$, (12) consists only of the first expression on the right. If d is a prime and $\equiv 1 \mod 4$, only T = d is possible on the right, and $E_d = E(q, d, d)_d$ is given in Proposition 3.

3. Further applications of the principle. Finally, we allow q to be an arbitrary odd prime. We consider pairs (ω_1, ω_2) in K(q) with $\omega_1^2 = -d_1$, $\omega_2^2 = -d_2$, d_1 and d_2 being square-free natural integers. We attach to them the order

$$\mathfrak{D} = (1, \, \omega_1, \, \omega_2, \, \frac{1}{2}(s + \Omega))$$

with $s = \omega_1 \omega_2 + \omega_2 \omega_1$ and $\Omega = \omega_1 \omega_2 - \omega_2 \omega_1$. A necessary condition that (ω_1, ω_2) lies in a maximal order of K(q) is: $\left(\frac{-d_1}{q}\right) \neq 1$, $\left(\frac{-d_2}{q}\right) \neq 1$ and

 $4d_1d_2-s^2$ is divisible by q an odd number of times. This condition is not satisfied if $4d_1d_2 < q$.

Theorem 3. If $4d_1d_2 < q$, no order of K(q) contains two elements ω_1, ω_2 with $\omega_1^2 = -d_1, \ \omega_2^2 = -d_2$.

The number of maximal orders of K(q) which contain the above order $\mathfrak D$ can be determined as in Section 2. This leads for q=2,3,5,7,13 to formulas for the products of class numbers $h(\sqrt{-d_1}) h(\sqrt{-d_2})$.

If we take $\omega_2 = f\omega_1$ with a natural number f and assume ω_2 to be optimally imbedded, we shall obtain infinitely many more formulas for $h(\omega)$ since $h(f\omega)/h(\omega)$ is known.

Finally, it can be mentioned that analogues of our theorems also hold for totally imaginary extensions of totally real fields.