[12] R. J. Miech, *A number theoretic constant*, Acta Arith. 15 (1968), pp. 119–137.
[13] L. J. Mordell, *On the Riemann hypothesis and imaginary quadratic fields with a given class number*, J. London Math. Soc. 9 (1934), pp. 289–298.
[14] A. Page, *On the number of primes in an arithmetic progression*, Proc. London Math. Soc. 39 (1935), pp. 116–141.
[15] G. Pólya, *Über die Verteilung der quadratischen Reste und Nichtreste*, Göttinger Nachrichten, 1918, pp. 21–29.
[16] W. M. Schmidt, *Zur Methode von Stepanov*, Acta Arith. 24 (1974), pp. 348–367.
[17] C. L. Siegel, *Über die Classenzahl quadratischer Zahlkörper*, Acta Arith. 1 (1935), pp. 83–86.
[18] P. J. Stephens, *Optimizing the size of $L(1, \chi)$*, Proc. London Math. Soc. (3) 24 (1972), pp. 1–14.
[19] T. Tatuzawa, *On a theorem of Siegel*, Japan J. Math. 21 (1951), pp. 163–178.
[20] A. Walfisz, *Zur additiven Zahlentheorie II*, Math. Zeitschr. 40 (1936), pp. 592–607.
[21] D. Wolke, *A note on the least prime quadratic residue* (mod p), Acta Arith. 16 (1969), pp. 85–87.

Received on 7. 2. 1975 (675)

ACTA ARITHMETICA
XXXI (1976)

On the arithmetic of quaternion algebras*

by

ARNOLD PIZER (Rochester, N. Y.)

Introduction. The purpose of this paper is to study the arithmetic of certain (in general) non-maximal orders in definite quaternion algebras over the rational numbers. They are the orders of level m, m a positive integer (see Definition 1). If $m = 1$, they are the maximal orders of the algebra and if m is square free they are the Eichler or hereditary orders and are studied in [3] and [6]. Our goal is to obtain explicit formulas for the "class number" of ideals associated to an order of level m (see Theorem 16) and the "type number" of orders of level m, i.e. the number of isomorphism classes of such orders (see Theorem 26).

1. Foundations. In this section we set our notation and give some basic facts and definitions. The basic reference for the arithmetic of quaternion algebras is [1] in which the reader will find proofs of the facts listed in this section.

$\mathfrak{A}$ will always denote a definite quaternion algebra over Q, the field of rational numbers, i.e. $\mathfrak{A}$ is a central simple algebra of dimension 4 over Q such that $\mathfrak{A} \otimes_Q \boldsymbol{R}$ is Hamilton's Quaternions. Here $\boldsymbol{R}$ denotes the field of real numbers.

For a finite prime p of Q, we let Q_p, v_p, $|\ |_p$ denote respectively the p-adic numbers, the normalized exponential valuation on Q_p, and the normalized valuation ($|a|_p = \left(\frac{1}{p}\right)^{v_p(a)}$) on Q_p. If A is any algebra over Q, $A_p = A \otimes_Q Q_p$ and A^* denotes the invertible elements of A. We also let $Q_\infty = \boldsymbol{R}$, $A_\infty = A \otimes_Q \boldsymbol{R}$, and call the absolute value in Q the infinite prime on Q. If I is any Z module contained in A, we let $I_p = I \otimes_Z Z_p$ where Z (Z_p) denotes the rational (resp. p-adic) integers. Finally, for any subring R of A (or of A_p), $U(R)$ denotes the units of R.

A prime p of Q is said to *ramify* (*split*) in $\mathfrak{A}$ if $\mathfrak{A}_p$ is a division algebra (resp. 2×2 matrices) over Q_p. The set of ramified primes is finite, even in number (if we count the infinite prime) and determines $\mathfrak{A}$ up to isomorphism.

* Written with partial support of NSF GP-42810.

We let $N(T)$ denote the reduced norm (resp. Trace) from $\mathfrak{A}$ to Q or from $\mathfrak{A}_p$ to Q_p. Thus $\mathfrak{A}$ is definite is equivalent to N being a positive definite quadratic form on $\mathfrak{A}$.

A *lattice* on $\mathfrak{A}$ is a finitely generated Z-module containing a base of $\mathfrak{A}$ over Q. An order of $\mathfrak{A}$ is a lattice on $\mathfrak{A}$ which is also a subring $\ni 1$. The obvious analogous definitions hold for lattices and orders in $\mathfrak{A}_p$, $p < \infty$ (i.e. p a finite prime). There is a local-global correspondence between lattices (and orders) which goes as follows (see [7]): To a lattice L on $\mathfrak{A}$, we associate the collection of lattices $L_p = L \otimes_Z Z_p$, one for each prime $p < \infty$. Conversely, if we have a collection of lattices $L(p)$ on $\mathfrak{A}_p$, one for each $p < \infty$, and if there exists a lattice M on $\mathfrak{A}$ such that $L(p) = M_p$ for almost all p, then there exists a unique lattice L $(= \bigcap_p L(p))$ on $\mathfrak{A}$ such that $L(p) = L_p$ for all $p < \infty$. Replacing the word "lattice" by "order" above, we get the local-global correspondence for orders. An order of $\mathfrak{A}$ (or $\mathfrak{A}_p$) is said to be *maximal* if it is not properly contained in any other order of $\mathfrak{A}$ (or $\mathfrak{A}_p$). M is a maximal order of $\mathfrak{A}$ if and only if M_p is maximal for all $p < \infty$. If $\mathfrak{A}_p$ is a division algebra ($p < \infty$), there exists a unique maximal order $= \{x \in \mathfrak{A}_p \mid N(x) \in Z_p\}$. If $\mathfrak{A}_p$ is split, all maximal orders are conjugate to the order $\begin{pmatrix} Z_p & Z_p \\ Z_p & Z_p \end{pmatrix}$. Let M be any maximal order of $\mathfrak{A}$. Then for p split, $\mathfrak{A}_p$ is isomorphic to 2×2 matrices over Q_p and by choosing an appropriate isomorphism, we can and do assume that $M_p = \begin{pmatrix} Z_p & Z_p \\ Z_p & Z_p \end{pmatrix}$. Thus we assume from now on that $\mathfrak{A}_p$ for p split is identified with 2×2 matrices over Q_p in such a way that there exists a maximal order M of $\mathfrak{A}$ with $M_p = \begin{pmatrix} Z_p & Z_p \\ Z_p & Z_p \end{pmatrix}$ for all split p.

DEFINITION 1. Let $\mathfrak{A}$ be a definite quaternion algebra over Q. Let q be the product of the finite primes of Q which ramify in $\mathfrak{A}$. Let m be a positive integer prime to q. An order M of $\mathfrak{A}$ is said to be of *level* m if M_p is maximal for all $p \mid q$ and M_p is isomorphic (i.e. conjugate) to $\begin{pmatrix} Z_p & Z_p \\ mZ_p & Z_p \end{pmatrix}$ for all $p \nmid q$, $p < \infty$.

By our above assumption, there exists a unique order $\mathfrak{O}$ of level m such that $\mathfrak{O}_p = \begin{pmatrix} Z_p & Z_p \\ mZ_p & Z_p \end{pmatrix}$ for all $p \nmid q$. We call this (by abuse of language) the canonical order of level m in $\mathfrak{A}$. For the remainder of this paper, $\mathfrak{O}$ will always denote this order.

DEFINITION 2. The *type number* of orders of level m in $\mathfrak{A}$ is the number of isomorphism classes of orders of level m in $\mathfrak{A}$. We denote this type number by T_{qm}.

DEFINITION 3. Let M be an order of level m on $\mathfrak{A}$. A *left M-ideal* is a lattice I on $\mathfrak{A}$ such that $I_p = M_p a_p$ (for some $a_p \in \mathfrak{A}_p^*$) for all $p < \infty$. Two left M-ideals I and J are said to be in the same *class* if $I = Ja$ for some $a \in \mathfrak{A}^*$. One has obviously the analogous concept of right ideals.

DEFINITION 4. The *class number* of (left) ideals for any order (M) of level m is the number of distinct classes of such ideals. We denote this class number by H_{qm}.

We will see in the next section that the type and class numbers are finite and that the class number depends only on the level, not on the particular order or on left or right ideals.

2. Class and type numbers. Let $\mathfrak{A}$ be as above and M any order, of $\mathfrak{A}$. The *idele* group $J_{\mathfrak{A}}$ of $\mathfrak{A}$ is

$$J_{\mathfrak{A}} = \left\{ \tilde{a} = (a_p) \in \prod_p \mathfrak{A}_p^* \mid a_p \in U(M_p) \text{ for almost all } p \right\}.$$

Here the product is over all primes (finite and infinite). Note that since given two orders M and N of $\mathfrak{A}$, $M_p = N_p$ for almost all p, $J_{\mathfrak{A}}$ is independent of the particular order used in its definition. $J_{\mathfrak{A}}$ is a locally compact group with the topology induced by the product topology on the open sets $\prod_{p \in S} \mathfrak{A}_p^* \prod_{p \notin S} U(M_p)$ where S ranges over all finite subsets of primes containing ∞. If $\tilde{a} = (a_p) \in J_{\mathfrak{A}}$, we define the volume of $\tilde{a}$ as

$$v(\tilde{a}) = \prod_p |N(a_p)|_p.$$

Let $J_{\mathfrak{A}}^1 = \{\tilde{a} \in J_{\mathfrak{A}} \mid v(\tilde{a}) = 1\}$ and embed $\mathfrak{A}^* \subseteq J_{\mathfrak{A}}^1$ along the diagonal. Finally if N is an order of level m of $\mathfrak{A}$, let

$$\mathfrak{U}(N) = \{\tilde{a} = (a_p) \in J_{\mathfrak{A}}^1 \mid a_p \in U(N_p) \text{ for all } p < \infty\}.$$

Then we have

PROPOSITION 5. 1) *$\mathfrak{A}^*$ is a discrete subgroup of $J_{\mathfrak{A}}^1$*, 2) *$J_{\mathfrak{A}}^1/\mathfrak{A}^*$ is compact*, 3) *$\mathfrak{U}(N)$ is an open compact subgroup of $J_{\mathfrak{A}}^1$.*

Proof. See Weil [11].

Now let q be the product of the finite ramified primes of $\mathfrak{A}$ and let m be a positive integer prime to q. Fix $\mathfrak{O}$, the canonical order of level m in $\mathfrak{A}$. If I is a left $\mathfrak{O}$-ideal, then $I_p = \mathfrak{O}_p a_p$ for some $a_p \in \mathfrak{A}_p^*$ for all $p < \infty$ and $a_p \in U(\mathfrak{O}_p)$ for almost all p (since $I_p = \mathfrak{O}_p$ for almost all p). Thus there exists an element $\tilde{a} \in J_{\mathfrak{A}}^1$ with the pth component of $\tilde{a}$ equal to a_p for all $p < \infty$. Conversely, if $\tilde{a} = (a_p) \in J_{\mathfrak{A}}^1$, then by the local-global correspondence, there is a unique lattice I such that $I_p = \mathfrak{O}_p a_p$ for all $p < \infty$. Thus (via the local-global correspondence) we get a transitive action of $J_{\mathfrak{A}}^1$ on the left $\mathfrak{O}$-ideals:

$$\tilde{a} = (a_p): \; I \leftrightarrow \{I_p\} \to \{I_p a_p\} \leftrightarrow J$$

and we write $J = I\tilde{a}$. Under this action the isotopy subgroup of $\mathfrak{O}$ is $\mathfrak{U}(\mathfrak{O})$ and we have the

PROPOSITION 6. *The double cosets* $\mathfrak{U}(\mathfrak{O})\backslash J^1_{\mathfrak{A}}/\mathfrak{A}^*$ *are in* 1-1 *correspondence with the ideal classes of left* $\mathfrak{O}$*-ideals.*

Proof. If $J^1_{\mathfrak{A}} = \bigcup_{\nu=1}^{H} \mathfrak{U}(\mathfrak{O})\tilde{a}_\nu\mathfrak{A}^*$, then $\mathfrak{O}\tilde{a}_\nu$, $\nu = 1, \ldots, H = H_{qm}$ represent the distinct $\mathfrak{O}$-ideal classes.

We also have the

PROPOSITION 7. $J^1_{\mathfrak{A}}$ *acts transitively (by conjugation) on orders of level* m *of* $\mathfrak{A}$.

Proof. The action is: For $\tilde{a} = (a_p) \in J^1_{\mathfrak{A}}$ and M an order of level m:

$$M \leftrightarrow \{M_p\} \to \{a_p^{-1} M_p a_p\} \leftrightarrow N$$

and we write $N = \tilde{a}^{-1}M\tilde{a}$. The action is obviously transitive by the definition of orders of level m.

PROPOSITION 8. 1) *The class number* H_{qm} *is finite and independent of the particular order (of level* m*) used in its definition. It is also the same for left or right ideals.*

2) *The type number* T_{qm} *satisfies* $T_{qm} \leqslant H_{qm}$. *In particular, it is finite.*

Proof. 1) H_{qm} (say for $\mathfrak{O}$) is the number of points in the space $\mathfrak{U}(\mathfrak{O})\backslash J^1_{\mathfrak{A}}/\mathfrak{A}^*$. But this is a compact discrete space, hence H_{qm} is finite. If $\mathfrak{O}\tilde{a}_1, \ldots, \mathfrak{O}\tilde{a}_H$, $H = H_{qm}$ represent the distinct left $\mathfrak{O}$ ideal classes, then $\tilde{a}_1^{-1}\mathfrak{O}, \ldots, \tilde{a}_H^{-1}\mathfrak{O}$ represent the distinct right ideal classes. If M is another order of level m with (say) $M = \tilde{b}^{-1}\mathfrak{O}\tilde{b}$, then $\tilde{b}^{-1}\mathfrak{O}\tilde{a}_1, \ldots, \tilde{b}^{-1}\mathfrak{O}\tilde{a}_H$ represent all the distinct left M-ideal classes.

2) Let $\mathfrak{O}\tilde{a}_1, \ldots, \mathfrak{O}\tilde{a}_H$ be as in 1) above. Then any order M of level m is easily seen to be of the same type as (at least) one of the right orders of the $\mathfrak{O}\tilde{a}_i$, i.e. $\tilde{a}_i^{-1}\mathfrak{O}\tilde{a}_i$. Thus $T_{qm} \leqslant H_{qm}$. Note that equality does not hold in general and compare with the proof of Lemma 32.

DEFINITION 9. If M is an order of $\mathfrak{A}$, the *normalizer* of M in $J^1_{\mathfrak{A}}$ is

$$\{\tilde{a} \in J^1_{\mathfrak{A}} \mid \tilde{a}^{-1}M\tilde{a} = M\}$$

and is denoted by $\mathfrak{N}(M)$.

We will need the

PROPOSITION 10. *Let* $\mathfrak{O}$ *be the canonical order of level* m *in* $\mathfrak{A}$. *Then*

$$[\mathfrak{N}(\mathfrak{O}) \colon \mathfrak{U}(\mathfrak{O})J^1_Q] = 2^e$$

where e *is the number of distinct primes dividing* qm. *More specifically: For* $p \mid q$, *let* π_p *be an element of* $\mathfrak{A}_p$ *with* $N(\pi_p) = p$. *For* $p \mid m$, *let*

$$\pi_p = \begin{pmatrix} 0 & 1 \\ p^r & 0 \end{pmatrix} \quad \text{with} \quad r = \nu_p(m).$$

Let $\tilde{\pi}_p = (a_l) \in J^1_{\mathfrak{A}}$ *be given by:* $a_l = 1$ *if* $l < \infty$, $l \neq p$, $a_l = \pi_p$ *if* $l = p$ *and* $a_\infty \in \boldsymbol{R}^*$ *is chosen so* $\tilde{\pi}_p \in J^1_{\mathfrak{A}}$. *Then*

$$\{\tilde{\pi}_{p_1}^{f_1} \cdots \tilde{\pi}_{p_e}^{f_e} \mid f_1, \ldots, f_e = 0 \text{ or } 1\}$$

is a complete set of coset representatives of $\mathfrak{N}(\mathfrak{O})$ mod $\mathfrak{U}(\mathfrak{O})J^1_Q$ *where* $p_1, \ldots, p_e$ *are the distinct primes dividing* qm.

Proof. This follows easily from local considerations. If $p \mid q$, all elements of $\mathfrak{A}_p^*$ normalize $\mathfrak{O}_p$ and $[\mathfrak{A}_p^* \colon U(\mathfrak{O}_p)Q_p^*] = 2$ with $\pi_p \notin U(\mathfrak{O}_p)Q_p^*$. If $p \nmid qm$, it is easy to see that the normalizer of $\mathfrak{O}_p$ in $\mathfrak{A}_p$ is just $U(\mathfrak{O}_p)Q_p^*$. If $p \mid m$, noting that $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in \mathfrak{O}_p$, we see easily that the only maximal orders containing $\mathfrak{O}_p$ are

$$\begin{pmatrix} Z_p & p^{-s}Z_p \\ p^s Z_p & Z_p \end{pmatrix} \quad \text{for} \quad s = 0, 1, \ldots, r.$$

Thus $\mathfrak{O}_p$ is the intersection of two unique maximal orders,

$$\mathfrak{O}_p = \begin{pmatrix} Z_p & Z_p \\ Z_p & Z_p \end{pmatrix} \cap \begin{pmatrix} Z_p & p^{-r}Z_p \\ p^r Z_p & Z_p \end{pmatrix}$$

and $a_p \in \mathfrak{A}_p^*$ normalizes $\mathfrak{O}_p$ if and only if conjugation by a_p permutes these two maximal orders, i.e. a_p normalizes $\mathfrak{O}_p$ if and only if $a_p \in U(\mathfrak{O}_p)Q_p^*$ or $a_p \in \pi_p U(\mathfrak{O}_p)Q_p^*$.

3. Optimal embeddings. The following question will be central to our study. Let K be a quadratic field extension of Q contained in $\mathfrak{A}$. If $\mathfrak{o}$ is an order of K and M is an order of $\mathfrak{A}$, we say that $\mathfrak{o}$ is *optimally embedded* in M if $K \cap M = \mathfrak{o}$. We ask: In how many essentially different orders M of level m can we optimally embed an order $\mathfrak{o}$ of K? If $m = 1$, the answer is 0 or 1 depending on whether the conductor of $\mathfrak{o}$ is prime to q or not — this is a special case of the Chevalley–Hasse–Noether Theorem. If m is square free, the answer is again 0 or 1 as was shown by Eichler ([3] and [4]). The solution of the general problem is due to Hijikata ([5]).

We first note the important trivial equivalence:

$$K \cap M = \mathfrak{o} \Leftrightarrow K_p \cap M_p = \mathfrak{o}_p \quad \text{for all } p < \infty.$$

Also any order M of level m can be written as $M = \tilde{b}^{-1}\mathfrak{O}\tilde{b}$ with $\tilde{b} = (b_p) \in J^1_{\mathfrak{A}}$ and $\mathfrak{O}$ the canonical order of level m. Suppose $K \cap \tilde{b}^{-1}\mathfrak{O}\tilde{b} = \mathfrak{o}$. If $\tilde{c} \in \mathfrak{N}(\mathfrak{O})$, then $K \cap \tilde{b}^{-1}\tilde{c}^{-1}\mathfrak{O}\tilde{c}\tilde{b} = \mathfrak{o}$, so we need only consider $\tilde{b} \in J^1_{\mathfrak{A}}$ mod $\mathfrak{N}(\mathfrak{O})$. Further if $\tilde{a} \in J^1_K$, then we have

$$K \cap \tilde{a}^{-1}\tilde{b}^{-1}\mathfrak{O}\tilde{b}\tilde{a} = \tilde{a}^{-1}\mathfrak{o}\tilde{a} = \mathfrak{o},$$

i.e. if $\mathfrak{o}$ is optimally embedded in M, it is optimally embedded in $\tilde{a}^{-1}M\tilde{a}$

for all $\tilde{a} \in J_K^1$ and we will consider these embeddings as being essentially the same. Thus we have the

DEFINITION 11. Let $\mathfrak{o}$, K, and $\mathfrak{A}$ be as above. Then $D(\mathfrak{o})$ will denote the number of double cosets $\mathfrak{N}(\mathfrak{O})\tilde{b}J_K^1$ in $J_{\mathfrak{A}}^1$ such that $K \cap \tilde{b}^{-1}\mathfrak{O}\tilde{b} = \mathfrak{o}$. $D(\mathfrak{o})$ is the number of essentially different orders (of level m) of $\mathfrak{A}$ in which $\mathfrak{o}$ is optimally embedded.

Locally, this reduces to

DEFINITION 12. Let $\mathfrak{o}, K, \mathfrak{A}$ be as above. Then $D(\mathfrak{o}_p)$ will denote the number of double cosets $N(\mathfrak{O}_p)b_pK_p^*$ in $\mathfrak{A}_p^*$ such that $K_p \cap b_p^{-1}\mathfrak{O}_p b_p = \mathfrak{o}_p$. Here

$$N(\mathfrak{O}_p) = \{a_p \in \mathfrak{A}_p^* \mid a_p^{-1}\mathfrak{O}_p a_p = \mathfrak{O}_p\}.$$

We now determine the numbers $D(\mathfrak{o}_p)$. There are three cases:

Case $p \mid q$: $K_p \cap \mathfrak{O}_p$ is the maximal order of K_p and $N(\mathfrak{O}_p) = \mathfrak{A}_p^*$. Thus $D(\mathfrak{o}_p) = 1$ or 0 according as $\mathfrak{o}_p$ is maximal in K_p or not.

Case $p \nmid qm$: Chevalley–Hasse–Noether implies $D(\mathfrak{o}_p) = 1$ always. This is easy to prove, see [4], p. 97 for example.

Case $p \mid m$: We follow Hijikata ([5]). Note first that

$$K_p \cap b_p^{-1}\mathfrak{O}_p b_p = \mathfrak{o}_p \Leftrightarrow b_p K_p b_p^{-1} \cap \mathfrak{O}_p = b_p \mathfrak{o}_p b_p^{-1}.$$

An isomorphism φ of K_p into $\mathfrak{A}_p$ is called an *optimal embedding* of $\mathfrak{o}_p/K_p$ into $\mathfrak{O}_p/\mathfrak{A}_p$ if $\varphi(K_p) \cap \mathfrak{O}_p = \varphi(\mathfrak{o}_p)$. If H is a subgroup of $N(\mathfrak{O}_p)$, we say two optimal embeddings φ and φ' are *equivalent* mod H and write $\varphi \sim \varphi' \pmod{H}$ if there exists $h \in H$ such that

$$\varphi'(x) = h\varphi(x)h^{-1} \quad \text{for all } x \in K_p.$$

For us H will always denote either $N(\mathfrak{O}_p)$ or $U(\mathfrak{O}_p)$. If $K_p \subseteq \mathfrak{A}_p$, it is obvious that there is a 1-1 correspondence between optimal embeddings of $\mathfrak{O}_p/K_p$ into $\mathfrak{O}_p/\mathfrak{A}_p$ mod $N(\mathfrak{O}_p)$ and double cosets $N(\mathfrak{O}_p)b_pK_p^*$ satisfying $K_p \cap b_p^{-1}\mathfrak{O}_p b_p = \mathfrak{o}_p$. Thus $D(\mathfrak{o}_p)$ is the number of equivalence classes of optimal embedding and Hijikata's result is (see [5]).

THEOREM 13. *Let $\mathfrak{A}_p, \mathfrak{O}_p$ be as above and assume $p \mid m$. Let $g \in \mathfrak{O}_p$, $g \notin Z_p$ have minimal polynomial $f(x) = x^2 - tx + n$ over Q_p. Let Λ be an order of $Q_p(g) = K$ containing g with $[\Lambda\colon Z_p + Z_p g] = p^q$. Finally let $r = v_p(m)$.*

Let Φ be the set of all solutions in $Z_p \pmod{p^{r+2q}}$ of the simultaneous equations $f(x) \equiv 0 \pmod{p^{r+2q}}$ and $2x - t \equiv 0 \pmod{p^q}$. Let $\Psi \subseteq \Phi$ be a complete set of representatives of $\Phi \bmod p^{r+q}$ (i.e. if $\xi' \in \Phi$, there exists $\xi \in \Psi$ such that $\xi' \equiv \xi \pmod{p^{r+q}}$ and if $\xi, \xi' \in \Psi$, $\xi \equiv \xi' \bmod p^{r+q} \Rightarrow \xi = \xi'$).

For $\xi \in \Psi$, let

$$\varphi_\xi(g) = \begin{pmatrix} \xi & p^q \\ -p^{-q}f(\xi) & t - \xi \end{pmatrix}.$$

Then φ_ξ induces an optimal embedding of $\Lambda/Q_p(g) \to \mathfrak{O}_p/\mathfrak{A}_p$ and any optimal embedding is $N(\mathfrak{O}_p)$ equivalent to some $\varphi_\xi(g)$.

Further for $\xi, \xi' \in \Psi$, we have:

if $p^{-2q}(t^2 - 4n)$ is a unit, then

$$\varphi_\xi \sim \varphi_{\xi'} \pmod{N(\mathfrak{O}_p)} \Leftrightarrow \xi \equiv t - \xi' \pmod{p^{r+q}};$$

if $p^{-2q}(t^2 - 4n)$ is not a unit, then

$$\varphi_\xi \sim \varphi_{\xi'} \pmod{N(\mathfrak{O}_p)} \Leftrightarrow \xi \equiv t - \xi' \pmod{p^{r+q}}$$
$$\text{and} \quad f(\xi') \not\equiv 0 \pmod{p^{r+2q+1}}.$$

(Note: *since $p \mid p^{-2q}(t^2 - 4n)$, this last condition is well defined.*)

Sketch of proof. Hijikata's idea is as follows. Suppose $\Lambda = Z_p + Z_p g$, i.e. $q = 0$. Let φ be an optimal embedding. Then $\varphi(g) \in \mathfrak{O}_p$ and by conjugation by elements of $N(\mathfrak{O}_p)$, we can assume the $(1, 2)$ entry in $\varphi(g)$ is 1, i.e. we assume

$$\varphi(g) = \varphi_\xi(g) = \begin{pmatrix} \xi & 1 \\ -f(\xi) & t - \xi \end{pmatrix}$$

where ξ is some element of Z_p. As $\varphi_\xi(g) \in \mathfrak{O}_p$, we must have $f(\xi) \equiv 0 \pmod{p^r}$. It is easy to see that $\varphi_\xi \sim \varphi_{\xi'} \pmod{U(\mathfrak{O}_p)}$ if and only if $\xi \equiv \xi' \pmod{p^r}$. A little work gives a set of distinct representatives mod $N(\mathfrak{O}_p)$. If $q > 0$, the procedure is more complicated, but the idea is the same. For the complete proof, see Hijikata [5], Theorem 2.3.

PROPOSITION 14. $D(\mathfrak{o}) = \prod_{p < \infty} D(\mathfrak{o}_p)$.

Proof. This is obvious.

4. The Selberg Trace Formula. Let G be a locally compact group with an open compact subgroup U and a discrete subgroup Γ with G/Γ compact. Then G is unimodular (i.e. every left Haar measure is a right Haar measure (see [8])) and we normalize Haar measure dx on G such that $\int_U dx = 1$. Let $L(G, U)$ be the set of complex valued continuous functions F on G with compact support such that $F(ugu') = F(g)$ for all $g \in G$, $u, u' \in U$. Let $L(U \backslash G / \Gamma)$ be the set of all complex valued continuous functions f of G such that $f(ug\gamma) = f(g)$ for all $u \in U$, $g \in G$, $\gamma \in \Gamma$. For any $\gamma \in \Gamma$, let $\{\gamma\}$ denote the conjugacy class of γ in Γ and let $\Gamma(\gamma)$ denote the centralizer of γ in Γ. For a discrete subgroup S of G, we also denote by dx the invariant quotient measure on G/S, i.e. if f is continuous with compact support on G, then

$$\int_G f(x)\,dx = \int_{H/S} \left(\sum_{s \in S} f(xs) \right) dx.$$

Any $F \in L(U \backslash G / \Gamma)$ induces a linear transformation on the finite dimensional complex vector space $L(U \backslash G / \Gamma)$ by convolution,

$$\big(F(f)\big)(x) = (F * f)(x) = \int_G F(xy^{-1}) f(y)\, dy$$

and its trace is given by

PROPOSITION 15 (Selberg Trace Formula).

$$\text{Trace } F = \sum_{\{\gamma\}} \int_{H/\Gamma(\gamma)} \psi_\gamma(x)\, dx$$

where $\psi_\gamma(x) = F(x\gamma x^{-1})$ *and the sum is over representatives of all conjugacy classes in* Γ.

Proof. See [9] and [10].

5. The class number. We seek a formula for the class number H_{qm}. Let us first state the result.

THEOREM 16. *Let* $\mathfrak{A}$ *be a definite quaternion algebra over* Q. *Let* q *be the product of the finite ramified primes of* $\mathfrak{A}$ *and let* m *be a positive integer prime to* q. *Then the class number* H_{qm} *of an order of level* m *in* $\mathfrak{A}$ *is*

$$H_{qm} = \frac{qm}{12} \prod_{p|q} \left(1 - \frac{1}{p}\right) \prod_{p|m} \left(1 + \frac{1}{p}\right) +$$

$$+ \begin{cases} \frac{1}{4} \prod_{p|q} \left(1 - \left(\frac{-4}{p}\right)\right) \prod_{p|m} \left(1 + \left(\frac{-4}{p}\right)\right) & \text{if } 4 \nmid m, \\ 0 & \text{if } 4 \mid m, \end{cases}$$

$$+ \begin{cases} \frac{1}{3} \prod_{p|q} \left(1 - \left(\frac{-3}{p}\right)\right) \prod_{p|m} \left(1 + \left(\frac{-3}{p}\right)\right) & \text{if } 9 \nmid m, \\ 0 & \text{if } 9 \mid m. \end{cases}$$

Here $\left(\frac{*}{*}\right)$ *is the Kronecker symbol and the products are over distinct primes dividing* q *or* m.

Proof. The proof will be given after a series of lemmas and propositions. Note that by Proposition 8, it suffices to consider left ideals for the canonical order $\mathfrak{O}$ of level m. In order to simplify the typography, for the rest of this section we let $G = J^1_{\mathfrak{A}}$, $U = \mathfrak{U}(\mathfrak{O})$ and $\Gamma = \mathfrak{A}^*$.

LEMMA 17. *Let* F *be the characteristic function on* U. *Let* dx *be the measure on* G *normalized so that* $\int_U dx = 1$. *Then*

$$H_{qm} = \sum_{\{\gamma\}} \int_{G/\Gamma(\gamma)} \psi_\gamma(x)\, dx \tag{1}$$

where $\psi_\gamma(x) = F(x\gamma x^{-1})$.

Proof. G, Γ, and U satisfy the hypotheses of Proposition 15. Since $\int_U dx = 1$, it is easy to see that F induces the identity map on $L(U \backslash G / \Gamma)$.

Thus $\text{Trace } F = \dim L(U \backslash G / \Gamma) = |U \backslash G / \Gamma| = H_{qm}$ and we use the Selberg Trace Formula.

LEMMA 18. *If*

$$\int_{G/\Gamma(\gamma)} \psi_\gamma(x)\, dx \neq 0,$$

then $\gamma = \pm 1$ *or has minimal polynomial* $x^2 + 1$ *or* $x^2 \pm x + 1$.

Proof. $\psi_\gamma(x) = F(x\gamma x^{-1}) \neq 0$ for some

$$x \in G \Leftrightarrow x\gamma x^{-1} \in \mathfrak{U}(\mathfrak{O}) \Leftrightarrow \gamma \in \mathfrak{U}(x^{-1}\mathfrak{O}x) \cap \mathfrak{A}^* = U(x^{-1}\mathfrak{O}x).$$

Thus γ is a unit of some order of $\mathfrak{A}$. If $\gamma \in Q$, we have $\gamma = \pm 1$. If $\gamma \notin Q$, then $T(\gamma) \in Z$ and $N(\gamma)$ is a unit of Z. Thus the minimal polynomial of γ is $f(x) = x^2 - tx + n$ where $t \in Z$, $n = \pm 1$. If $f(x)$ had a real root, it would mean that $\boldsymbol{R}$ is a splitting field for $\mathfrak{A}$, contradicting the definiteness of $\mathfrak{A}$. Thus $t^2 - 4n < 0$, i.e. $n = 1$ and $t = 0$ or ± 1.

Since two elements of $\mathfrak{A}^*$ are conjugate if and only if they have the same minimal polynomial, we have determined all possible conjugacy classes which give a non-zero contribution to (1). We first calculate the contribution to (1) from $\gamma = \pm 1$.

LEMMA 19. *Let* $\mathfrak{O}$ *be a maximal order (i.e. assume* $m = 1$). *Then*

$$\text{vol}(G/\Gamma) = \frac{q}{24} \prod_{p|q} \left(1 - \frac{1}{p}\right).$$

Proof. Recall the measure dx is normalized so that $\text{vol}\big(\mathfrak{U}(\mathfrak{O})\big) = 1$.

$$G = J^1_{\mathfrak{A}} = \bigcup_{\nu=1}^{H_{q1}} \mathfrak{U}(\mathfrak{O}) g_\nu \mathfrak{A}^*$$

where $\mathfrak{O}g_\nu$, $\nu = 1, \ldots, H_{q1}$, represent all the left $\mathfrak{O}$-ideal classes.

$$\text{Vol}(G/\Gamma) = \sum_\nu \text{vol}\big(\mathfrak{U}(\mathfrak{O}) g_\nu \Gamma / \Gamma\big) = \sum_\nu \text{vol}\big(g_\nu^{-1}\mathfrak{U}(\mathfrak{O}) g_\nu \Gamma / \Gamma\big)$$

$$= \sum_\nu \text{vol}\big(\mathfrak{U}(g_\nu^{-1}\mathfrak{O}g_\nu) / \mathfrak{U}(g_\nu^{-1}\mathfrak{O}g_\nu) \cap \Gamma\big) = \sum_\nu \frac{1}{|U(g_\nu^{-1}\mathfrak{O}g_\nu)|}.$$

But $\sum_\nu \frac{1}{|U(g_\nu^{-1}\mathfrak{O}g_\nu)|}$ is by definition the Mass for $\mathfrak{O}$-ideals. Its value is

well known to be that given in the lemma. Its computation involves the evaluation of the residue of the zeta function of $\mathfrak{A}$ at 2 (or at 1 in Eichler's notation) by two different methods. See [2] and [4], p. 95.

PROPOSITION 20. *Let $\mathfrak{O}$ be an order of level m in $\mathfrak{A}$. Then the Mass formula is*:

$$\text{vol}(G/\Gamma) = \frac{qm}{24}\prod_{p|q}\left(1-\frac{1}{p}\right)\prod_{p|m}\left(1+\frac{1}{p}\right). \tag{2}$$

Proof. We assume $\mathfrak{O}$ is the canonical order of level m. Let $\mathfrak{O}'$ be the canonical order of level 1. Then $\mathfrak{O}\subseteq\mathfrak{O}'$ and

$$[\mathfrak{U}(\mathfrak{O}'):\mathfrak{U}(\mathfrak{O})] = \prod_{p}[U(\mathfrak{O}'_p):U(\mathfrak{O}_p)] = m\prod_{p|m}\left(1+\frac{1}{p}\right)$$

since

$$\left[U\begin{pmatrix}Z_p & Z_p\\ p^rZ_p & Z_p\end{pmatrix}:U\begin{pmatrix}Z_p & Z_p\\ p^{r+1}Z_p & Z_p\end{pmatrix}\right] = \begin{cases}p+1 & \text{if } r=0,\\ p & \text{if } r\geqslant 1.\end{cases}$$

Thus

$$\text{vol}\big(\mathfrak{U}(\mathfrak{O}')\big) = m\prod_{p|m}\left(1+\frac{1}{p}\right).$$

Lemma 19 gives the volume of G/Γ under the assumption $\text{vol}\big(\mathfrak{U}(\mathfrak{O}')\big)=1$ hence the volume of G/Γ in the present case is $m\prod_{p|m}\left(1+\frac{1}{p}\right)$ times as large.

Remark. The above proof works for definite quaternion algebras over any (totally real) number field and one gets the obvious generalization of Eichler's mass formula 12 in [3].

We now consider the computation of $\int_{G/\Gamma(\gamma)}\psi_\gamma(x)\,dx$ for $\gamma\neq\pm 1$.

LEMMA 21. *Assume $\gamma\neq\pm1$ and suppose $\psi_\gamma(x)$ is not identically zero. Let $K=Q(\gamma)$. Then the support of $\psi_\gamma(x)$ in G consists of the disjoint union of the double cosets $\mathfrak{N}(\mathfrak{O})\tilde{b}J^1_K$ satisfying $K\cap\tilde{b}^{-1}\mathfrak{O}\tilde{b}=\mathfrak{o}$ for some $\mathfrak{o}$ of K containing γ.*

Proof. $\psi_\gamma(\tilde{y})\neq 0\Rightarrow\tilde{y}\gamma\tilde{y}^{-1}\in\mathfrak{U}(\mathfrak{O})\Leftrightarrow\gamma\in K\cap\tilde{y}^{-1}\mathfrak{O}\tilde{y}=\mathfrak{o}$ (say). Conversely, if $K\cap\tilde{y}^{-1}\mathfrak{O}\tilde{y}=\mathfrak{o}\supset\gamma$ for some $\tilde{y}\in J^1_{\mathfrak{A}}$, then $\tilde{y}\gamma\tilde{y}^{-1}\in\mathfrak{U}(\mathfrak{O})$ (since $N(\gamma)=1$) $\Rightarrow\psi_\gamma(\tilde{y})=1$.

PROPOSITION 22. *Assume $\gamma\in\mathfrak{A}^*$, $\gamma\notin Q$ and the minimal polynomial of γ is $f(x)=x^2-sx+n$ with $s,n\in Z$. Let $K=Q(\gamma)$ and assume $K\cap\tilde{b}^{-1}\mathfrak{O}\tilde{b}=\mathfrak{o}\supset\gamma$ for some $\tilde{b}=(b_p)\in J^1_{\mathfrak{A}}$. Finally assume $\gamma\in\mathfrak{N}(\tilde{b}^{-1}\mathfrak{O}\tilde{b})$. Then $\mathfrak{N}(\mathfrak{O})\tilde{b}J^1_K$ consists of the disjoint union of $E(\mathfrak{o})$ translates of $\mathfrak{U}(\mathfrak{O})\tilde{b}J^1_K$ where $E(\mathfrak{o})=\prod_{p<\infty}E(\mathfrak{o}_p)$ and where:*

if $p\nmid qm$, $E(\mathfrak{o}_p)=1$;

if $p\mid q$, $E(\mathfrak{o}_p)=\begin{cases}1 & \text{if } p \text{ ramifies in } K,\\ 2 & \text{if } p \text{ remains prime in } K;\end{cases}$

if $p\mid m$, we let $v_p(m)=r$ and $[\mathfrak{o}_p: Z_p+Z_p\gamma]=p^\varrho$.

We can assume by Hijikata's Theorem 13 that

$$b_p\gamma b_p^{-1} = \begin{pmatrix}\xi & p^\varrho\\ -p^{-\varrho}f(\xi) & s-\xi\end{pmatrix} \quad \text{for some } \xi\in Z_p.$$

Then

$$E(\mathfrak{o}_p) = \begin{cases}1 & \text{if } \quad v_p\big(f(\xi)\big)=r+2\varrho \text{ and } v_p(s-2\xi)\geqslant r+\varrho,\\ 2 & \text{otherwise.}\end{cases}$$

Proof. $\mathfrak{N}(\mathfrak{O})=\bigcup\tilde{\pi}_{p_1}^{f_1}\dots\tilde{\pi}_{p_e}^{f_e}\mathfrak{U}(\mathfrak{O})J^1_Q$ where $f_1,\dots,f_e=0$ or 1 and $p_1,\dots,p_e$ are the distinct primes dividing qm by Proposition 10. Thus

$$\mathfrak{N}(\mathfrak{O})\tilde{b}J^1_K=\bigcup\tilde{\pi}_{p_1}^{f_1}\dots\tilde{\pi}_{p_e}^{f_e}\mathfrak{U}(\mathfrak{O})\tilde{b}J^1_K,\quad f_1,\dots,f_e=0 \text{ or } 1.$$

As the $\tilde{\pi}_{p_i}$ commute with each other one can see that we need only determine how many $\tilde{\pi}_{p_i}$ are absorbed into $\mathfrak{U}(\mathfrak{O})\tilde{b}J^1_K\tilde{b}^{-1}$. But

$$\tilde{\pi}_p\in\mathfrak{U}(\mathfrak{O})\tilde{b}J^1_K\tilde{b}^{-1}\Leftrightarrow\pi_p\in U(\mathfrak{O}_p)b_pK_p^*b_p^{-1}.$$

For $p\mid q$, $\pi_p\in U(\mathfrak{O}_p)b_pK_p^*b^{-1}\Leftrightarrow p$ ramifies in K (see [6], Lemma 13). Note that p can not split in K^p for that would imply $\mathfrak{A}_p$ is split. For $p\mid m$,

$$\pi_p=\begin{pmatrix}0 & 1\\ p^r & 0\end{pmatrix}\in U(\mathfrak{O}_p)b_pK_p^*b_p^{-1}=U(\mathfrak{O}_p)\big(Q_p+Q_p(b_p\gamma b_p^{-1})\big)$$

if and only if

$$\begin{pmatrix}u & a\\ bp^r & v\end{pmatrix}\begin{pmatrix}0 & 1\\ p^r & 0\end{pmatrix}=\begin{pmatrix}ap^r & u\\ vp^r & bp^r\end{pmatrix}=x\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}+y\begin{pmatrix}\xi & p^\varrho\\ -p^{-\varrho}f(\xi) & s-\xi\end{pmatrix}$$

for some u,v units of Z_p, $a,b\in Z_p$ and $x,y\in Q_p$. Thus $\pi_p\in U(\mathfrak{O}_p)b_pK_p^*b_p^{-1}$ implies $v_p\big(f(\xi)\big)=r+2\varrho$ and $v_p(s-2\xi)\geqslant r+\varrho$. Conversely if $v_p\big(f(\xi)\big)=r+2\varrho$ and $v_p(s-2\xi)\geqslant r+\varrho$, then there exists $x\in Q_p$ such that

$p^{-\varrho}\xi + x \equiv p^{-\varrho}(s-\xi)+x \equiv 0 \pmod{p^r}$. Then

$$x + p^{-\varrho}\begin{pmatrix} \xi & p^{\varrho} \\ -p^{-\varrho}f(\xi) & s-\xi \end{pmatrix} = \begin{pmatrix} ap^r & 1 \\ vp^r & bp^r \end{pmatrix}$$

for some $a, b \in Z_p$ and v a unit of Z_p. Hence $\pi_p \in U(\mathfrak{O}_p) b_p K_p^* b_p^{-1}$ and the proposition is proved.

We obviously need the

LEMMA 23. *Let $\gamma, K, \tilde{b}, \mathfrak{o}$ be as in Proposition 22. Then*

$$\mathrm{vol}\big(\mathfrak{U}(\mathfrak{O})\tilde{b}J_K^1/K^*\big) = \frac{h(\mathfrak{o})}{w(\mathfrak{o})}$$

where $h(\mathfrak{o})$ is the class number of locally principal $\mathfrak{o}$-ideals in K, i.e.

$$h(\mathfrak{o}) = |J_K^1/\mathfrak{U}(\mathfrak{o})K^*|$$

where $\mathfrak{U}(\mathfrak{o}) = \mathfrak{U}(\mathfrak{O}) \cap J_K^1 = \big(\prod_{p<\infty} U(\mathfrak{o}_p) \times K_\infty^*\big) \cap J_K^1$ and $w(\mathfrak{o}) = |U(\mathfrak{o})|$. The volume is taken with respect to the quotient measure on $J_{\mathfrak{A}}^1/K^*$.

Proof. Let $J_K^1 = \bigcup_{i=1}^{h(\mathfrak{o})} \tilde{x}_i \mathfrak{U}(\mathfrak{o}) K^*$ (disjoint.) Then

$$\mathrm{vol}\big(\mathfrak{U}(\mathfrak{O})\tilde{b}J_K^1/K^*\big) = \mathrm{vol}\big(\mathfrak{U}(\tilde{b}^{-1}\mathfrak{O}\tilde{b})J_K^1/K^*\big) = \mathrm{vol}\Big(\bigcup_{i=1}^{h(\mathfrak{o})} \big(\tilde{x}_i^* \mathfrak{U}(\tilde{b}^{-1}\mathfrak{O}\tilde{b})K^*/K^*\big)\Big)$$

$$= h(\mathfrak{o})\,\mathrm{vol}\big(\mathfrak{U}(\tilde{b}^{-1}\mathfrak{O}\tilde{b})/\mathfrak{U}(\tilde{b}^{-1}\mathfrak{O}\tilde{b}) \cap K^*\big) = \frac{h(\mathfrak{o})}{w(\mathfrak{o})}.$$

PROPOSITION 24. *Let γ, K be as in Lemma 21 and let $\mathfrak{o}$ be a fixed order of K containing γ. Then $\Gamma(\gamma) = K^*$ and the volume in $G/\Gamma(\gamma)$ of the support of $\psi_\gamma(x)$ attached to $\mathfrak{o}$, i.e. the sum of the volumes of $\mathfrak{N}(\mathfrak{O})\tilde{b}J_K^1/K^*$ over all double cosets satisfying $K \cap \tilde{b}^{-1}\mathfrak{O}\tilde{b} = \mathfrak{o}$ is $D(\mathfrak{o})E(\mathfrak{o})\dfrac{h(\mathfrak{o})}{w(\mathfrak{o})}$.*

Proof. It is well known that the centralizer of γ in $\mathfrak{A}^*$ is just $Q(\gamma)^* = K^*$. The rest follows immediately from Definition 11, Lemmas 21 and 23, and Proposition 22.

Proof of Theorem 16. We evaluate (1). By Lemma 18 we need only consider $\gamma = \pm 1$ and γ a root of x^2+1 or $x^2 \pm x + 1$. If $\gamma = \pm 1$, $\Gamma(\gamma) = \Gamma$ and

$$\int_{G/\Gamma(\gamma)} \psi_\gamma(x)\,dx = \mathrm{vol}(G/\Gamma)$$

which is given by (2) and gives the first term of the formula for H_{qm}.

Now consider γ a root of x^2+1. Let $K = Q(\gamma)$ and assume K is embedded in $\mathfrak{A}$. By Lemma 21 and Proposition 24 we must consider all orders $\mathfrak{o}$ of K containing γ and for each such order compute $D(\mathfrak{o})E(\mathfrak{o})\dfrac{h(\mathfrak{o})}{w(\mathfrak{o})}$. As γ generates the maximal order of K, we need only consider $\mathfrak{o} = Z + Z\gamma$. It is well known that $h(\mathfrak{o}) = 1$ and $w(\mathfrak{o}) = 4$. We calculate $D(\mathfrak{o})$ and $E(\mathfrak{o})$.

If $p \nmid qm$, then $D(\mathfrak{o}_p) = E(\mathfrak{o}_p) = 1$.

If $p \mid q$, then as $\mathfrak{o}_p$ is maximal, $D(\mathfrak{o}_p) = 1$ and $E(\mathfrak{o}_p) = \left(1 - \left(\dfrac{-4}{p}\right)\right)$.

Note $E(\mathfrak{o}_p) \neq 0$ as $K \subseteq \mathfrak{A}$.

If $p \mid m$, $p \neq 2$ we let the notation be as in Theorem 13 ($\Lambda = \mathfrak{o}_p$). As $\mathfrak{o}_p = Z_p + Z_p\gamma$, $\varrho = 0$. $x^2+1 \equiv 0 \pmod{p^r}$ has a solution in $Z_p \pmod{p^r}$ $\Leftrightarrow \left(\dfrac{-1}{p}\right) = 1$. If $\left(\dfrac{-1}{p}\right) = 1$, we have two solutions $\pm\xi$. $p^{-2\varrho}(t^2 - 4n)$ $= -4$ is a unit and $\xi \equiv 0 - (-\xi) \pmod{p^{r+\varrho}}$ implies there is only one equivalence class of optimal embeddings. Thus

$$D(\mathfrak{o}_p) = \begin{cases} 1 & \text{if} \quad \left(\dfrac{-4}{p}\right) = 1, \\ 0 & \text{if} \quad \left(\dfrac{-4}{p}\right) = -1. \end{cases}$$

If $D(\mathfrak{o}_p) = 1$, we have

$$v_p(t - 2\xi) = v_p(-2\xi) = 0 < 1 \quad \text{as} \quad N(\xi) = 1.$$

Thus by Proposition 22,

$$E(\mathfrak{o}_p) = 2 = \left(1 + \left(\frac{-4}{p}\right)\right).$$

If $2 \mid m$, again using the notation of Theorem 13, we have two cases: if $r = 1$, then $x^2+1 \equiv 0 \pmod 2$ has one solution $\xi = 1$. Thus $D(\mathfrak{o}_2) = 1$. $v_2(t - 2\xi) = 1$ and $v_2\big(f(1)\big) = 1$ implies $E(\mathfrak{o}_2) = 1 = \left(1 + \left(\dfrac{-4}{2}\right)\right)$; if $r \geqslant 2$, $x^2+1 \equiv 0 \pmod{2^r}$ has no solution so $D(\mathfrak{o}_2) = 0$. Thus $D(\mathfrak{o}) = 0$ or 1 and $D(\mathfrak{o}) = 1 \Leftrightarrow E(\mathfrak{o}) \neq 0$ and $4 \nmid qm$ in which case

$$E(\mathfrak{o}) = \prod_{p \mid q}\left(1 - \left(\frac{-4}{p}\right)\right) \prod_{p \mid m}\left(1 + \left(\frac{-4}{p}\right)\right).$$

Finally $K = Q(\gamma)$ can be embedded in $\mathfrak{A}$ if and only if K_p splits $\mathfrak{A}^p$ for all p (Brauer–Hasse–Noether Theorem) if and only if K is totally

imaginary and K_p is a quadratic field extension of Q_p for all $p \mid q$ if and only if $\prod_{p \mid q}\left(1-\left(\frac{-4}{p}\right)\right) \neq 0$. Thus if K can not be embedded in $\mathfrak{A}$, $E(\mathfrak{o})$ is already zero so our initial assumption that $K \subseteq \mathfrak{A}$ is no restriction. These considerations give the second term of H_{qm}.

Remark 25. The phenomenon explained in the above paragraph, that assuming $K \subseteq \mathfrak{A}$ is no restriction on the final formula will occur so often in the remaining calculations that we designate it "Remark 25" so that we can briefly call the reader's attention to it from time to time.

Now consider a root γ of $x^2 \pm x+1$ and let $K = Q(\gamma)$. As γ is a root of x^2+x+1 if and only if $-\gamma$ is a root of x^2-x+1 and since γ and $-\gamma$ both generate the same field K and the same order $Z+Z\gamma$ of K, we need consider only one, say γ, a root of x^2+x+1. Assume (Remark 25) that $K \subseteq \mathfrak{A}$ and note that $Z+Z\gamma = \mathfrak{o}$ is the maximal order of K. Again we need only compute

$$D(\mathfrak{o})E(\mathfrak{o})\frac{h(\mathfrak{o})}{w(\mathfrak{o})} = \frac{1}{6}D(\mathfrak{o})E(\mathfrak{o}).$$

If $p \nmid qm$,

$$D(\mathfrak{o}_p) = E(\mathfrak{o}_p) = 1.$$

If $p \mid q$,

$$D(\mathfrak{o}_p) = 1, \quad E(\mathfrak{o}_p) = \left(1-\left(\frac{-3}{p}\right)\right).$$

If $p \mid m$, $p \neq 2$, $p \neq 3$, we use the notation of Theorem 13. $x^2+x+1 \equiv 0 \pmod{p^r}$ has a solution $\Leftrightarrow \left(\frac{-3}{p}\right) = 1$. If $\left(\frac{-3}{p}\right) = 1$, there are two solutions $\xi = \frac{1}{2}\alpha - \frac{1}{2}$ and $\xi' = -\frac{1}{2}\alpha - \frac{1}{2}$ where $\alpha^2 \equiv -3 \pmod{p^r}$. $p^{-2q}(t^2-4n) = -3$ is a unit and $\xi \equiv t-\xi' \pmod{p^r}$ so

$$D(\mathfrak{o}_p) = \begin{cases} 0 & \text{if } \left(\frac{-3}{p}\right) = -1, \\ 1 & \text{if } \left(\frac{-3}{p}\right) = 1. \end{cases}$$

If $D(\mathfrak{o}_p) = 1$, $v_p(t-2\xi) = 0 < r \Rightarrow E(\mathfrak{o}_p) = 2 = \left(1+\left(\frac{-3}{p}\right)\right)$. If $2 \mid m$, $x^2+x+1 \equiv 0 \pmod 2$ has no solutions, i.e.

$$D(\mathfrak{o}_2) = 0 = \left(1+\left(\frac{-3}{2}\right)\right) \quad \text{if} \quad 2 \mid m.$$

If $3 \mid m$, there are two cases: $v_3(m) = 1 = r$ in which case $x^2+x+1 \equiv 0 \pmod 3$ has one solution, so $D(\mathfrak{o}_3) = 1$ and we see $E(\mathfrak{o}_3) = 1 = \left(1+\left(\frac{-3}{3}\right)\right)$ also; in the other case $r \geqslant 2$, $x^2+x+1 \equiv 0 \pmod{3^r}$ has no solution so $D(\mathfrak{o}_3) = 0$. Thus $D(\mathfrak{o}) = 0$ or 1 and $D(\mathfrak{o}) = 1$ if and only if

$$E(\mathfrak{o}) = \prod_{p \mid q}\left(1-\left(\frac{-3}{p}\right)\right)\prod_{p \mid m}\left(1+\left(\frac{-3}{p}\right)\right) \neq 0$$

and $9 \nmid qm$. Recalling we must consider both $\pm\gamma$, we get the third term of the formula for H_{qm}. This completes the proof of Theorem 16.

6. The type number. Let $\mathfrak{A}$ be a definite quaternion algebra over Q with q the product of the finite ramified primes of $\mathfrak{A}$ and m a positive integer prime to q. Before stating the formula for the type number T_{qm} of orders of level m in $\mathfrak{A}$, we introduce some notation which will remain in effect for the remainder of this section. First for any $a, b \in Z$ we write $a \| b$ to mean $a \mid b$ and $\left(a, \frac{b}{a}\right) = 1$. Secondly for any $s \in Z$, $s > 0$ we write s_1, s_2 to denote the unique positive integers with $s = s_1 s_2^2$ and s_1 square free (i.e. $v_p(s_1) = 0$ or 1 for all p).

THEOREM 26. *Assume $\mathfrak{A}$, q, m, etc. are as above. The type number is given by the formula*

$$T_{qm} = \frac{1}{2^e}H_{qm} + t_2 + t_3 + \sum_{\substack{s \geqslant 4 \\ s \| m}} t_s \tag{3}$$

where:

H_{qm} *is the class number given by Theorem* 16,

$$t_2 = \begin{cases} \frac{1}{2}\delta(8,1)+\frac{1}{2}\delta(4,1) & \text{if } 2 \| qm, \\ 0 & \text{if } 2 \nmid qm; \text{ or } 4 \mid qm; \end{cases}$$

$$t_3 = \begin{cases} \delta(3,1) & \text{if } 3 \| qm \text{ and } 2 \nmid qm, \\ \frac{1}{2}\delta(3,1) & \text{if } 3 \| qm \text{ and } 2 \mid q, \\ \frac{1}{3}\delta(3,1)+\delta(3,2) & \text{if } 3 \| qm \text{ and } 2 \text{ or } 4 \| m, \\ 0 & \text{if } 8 \mid m, \\ 0 & \text{if } 3 \nmid qm \text{ or } 9 \mid qm. \end{cases}$$

We consider two cases for t_s with $s = s_1 s_2^2$:

Case $s_1 \equiv 1$ *or* $2 \pmod 4$. *Then*

$$t_s = \begin{cases} 0 & \text{if } 4 \mid m \text{ and } 4 \nmid s, \\ \frac{1}{2}\delta(4s_1, s)h(-s) & \text{otherwise.} \end{cases}$$

Case $s_1 \equiv 3 \pmod 4$. *Then*

$$t_s = \begin{cases} \frac{1}{2}\delta(s_1,s)h(-s)\left(1+\dfrac{1}{2-\left(\frac{-s_1}{2}\right)}\right) & \text{if } 2\nmid qm, \\ \frac{1}{2}\delta(s_1,s)h(-s)\dfrac{1}{\left(2-\left(\frac{-s_1}{2}\right)\right)} & \text{if } 2\mid q, \\ \frac{1}{2}\delta(s_1,s)h(-s) & \text{if } 2\mid m \text{ and } 2\mid s, \\ \delta(s_1,2s)h(-s)+\frac{1}{2}\delta(s_1,s)h(-s)\dfrac{1}{\left(2-\left(\frac{-s_1}{2}\right)\right)} & \text{if } 2\parallel m \text{ and } 2\nmid s, \\ \frac{1}{2}\delta(s_1,2s)h(-s)\left(3+\left(\frac{-s_1}{2}\right)\right)+ & \\ \qquad +\frac{1}{2}\delta(s_1,s)h(-s)\dfrac{1}{\left(2-\left(\frac{-s_1}{2}\right)\right)} & \text{if } 4\parallel m \text{ and } 2\nmid s, \\ \frac{1}{2}\delta(s_1,s)h(-s)\left(3+\dfrac{1}{\left(2-\left(\frac{-s_1}{2}\right)\right)}\right) & \text{if } 8\mid m \text{ and } 2\nmid s. \end{cases}$$

Here:
e is the number of distinct primes dividing qm,

$$\delta(s,r) = \frac{1}{2^e}\prod_{p\mid q}\left(1-\left(\frac{-s}{p}\right)\right)\prod_{\substack{p\mid m\\ p\nmid r}}\left(1+\left(\frac{-s}{p}\right)\right),$$

$h(-s)$ = *class number of the order* $Z+Z\sqrt{-s}$ *in the field* $Q(\sqrt{-s})$ (see Lemma 44).

Proof. The idea of the proof is similar to that of Theorem 16 and the proof will proceed by a series of lemmas. We first note that $J^1_{\mathfrak{A}}$ acts transitively on orders of level m (Proposition 7) and the double cosets $\mathfrak{N}(\mathfrak{O})\backslash J^1_{\mathfrak{A}}/\mathfrak{A}^*$ are in 1-1 correspondence with types of orders of level m. However, $\mathfrak{N}(\mathfrak{O})$ is not compact so we have to consider

$$G = J^1_{\mathfrak{A}}/J^1_Q, \quad \Gamma = \mathfrak{A}^*J^1_Q/J^1_Q = \mathfrak{A}^*/Q^*, \quad \text{and} \quad U = \mathfrak{N}(\mathfrak{O})/J^1_Q$$

and we fix this notation for the remainder of this section. Under the quotient topology G remains a locally compact (unimodular) group, U is an open compact subgroup (by Proposition 10) and it is not hard to see that Γ is a discrete subgroup wih compact quotient G/Γ. As $T_{qm} = |U\backslash G/\Gamma|$ and G, U, Γ satisfy the hypothesis of the trace formula (Proposition 15) we have

Lemma 27. *Let F be the characteristic function on U. Let dx be the Haar measure on G normalized so that $\int_U dx = 1$. Then*

$$T_{qm} = \sum_{\{\gamma\}\subseteq\Gamma}\int_{G/\Gamma(\gamma)}\psi_\gamma(x)\,dx. \tag{4}$$

Proof. The proof is the same as that of Lemma 17.

We introduce the following notation: if $\gamma\in\Gamma = \mathfrak{A}^*/Q^*$ we write $\gamma \equiv a$ with $a\in\mathfrak{A}^*$ to mean that a is a representative of γ in $\mathfrak{A}^*$. As $\psi_\gamma(x) \neq 0 \Leftrightarrow \gamma \equiv a\in\mathfrak{N}(x^{-1}\mathfrak{O}x)$, we are interested in

Lemma 28. *If $\gamma\in\Gamma$, $\gamma\neq 1$ (i.e. $\gamma \equiv b\notin Q^*$) and $\gamma\in\mathfrak{N}(F)$ for some order F of level m, then $\gamma \equiv a$ for some $a\in F\cap\mathfrak{A}^*$ having minimal polynomial x^2-tx+n with $t, n\in Z$ and* (i) $n\parallel qm$; (ii) $n\mid t$; (iii) $t^2-4n<0$.

Proof. First assume $F=\mathfrak{O}$ and let γ normalize $\mathfrak{O}$ with $\gamma\equiv c\in\mathfrak{A}^*$. Then

if $p\nmid qm$, $c = u_p b_p$,
if $p\mid q$, $c = u_p\pi_p^{e_p}b_p$, $e_p = 0$ or 1,
if $p\mid m$, $c = u_p\pi_p^{e_p}b_p$, $e_p = 0$ or 1,

by the proof of Proposition 10. Here u_p is some unit of $\mathfrak{O}_p$, π_p is as in Proposition 10 and b_p is some element of Q_p^*. There exists $b\in Q^*$ and units $w_p\in U(Z_p)$ such that $b = b_p w_p$ for all $p<\infty$. Taking $a = cb^{-1}$, we have $\gamma\equiv a$ and $a\in\mathfrak{O}$ (as $a\in\mathfrak{O}_p$ for all p). The minimal polynomial of a, say $f(x) = x^2-tx+n$, satisfies $n, t\in Z$ and $n\parallel qm$. Now if $p\mid n$ and $p\mid q$, then $p\mid t$ by Hensel's Lemma ($p\nmid t \Rightarrow x^2-tx+n$ has a root in $Q_p \Rightarrow \mathfrak{A}_p$ is split). If $p\mid n$ and $p\mid m$ we must have $v_p(n) = v_p(m) = r$ (say). Then $a = u_p\begin{pmatrix}0 & 1\\ p^r & 0\end{pmatrix}$ and it is easy to see that $p^r\mid T(a)$. Thus $n\mid t$. Finally as $\mathfrak{A}$ is definite, $f(x)$ can have only complex roots, i.e. $t^2-4n<0$. As every order of level m is conjugate locally everywhere to $\mathfrak{O}$, the lemma is proved.

Lemma 29. *If $\gamma\in\Gamma$, $\gamma\neq 1$ normalizes an order of level m, then there exists $a\in\mathfrak{A}^*$ with $\gamma\equiv a$ such that the minimal polynomial of a is one of*

$$\begin{cases} x^2+1 \text{ or } x^2+x+1, & \\ x^2+2 \text{ or } x^2+2x+2 & \text{if } 2\parallel qm, \\ x^2+3 \text{ or } x^2+3x+3 & \text{if } 3\parallel qm, \\ x^2+n,\ n\geqslant 4 & \text{for } n\parallel qm. \end{cases} \tag{5}$$

Proof. Let a be as in Lemma 28. The minimum polynomial of a can be written as x^2-cn+n where $c\in Z$, $n\|qm$. $(cn)^2-4n<0$ implies $n>0$. Then $c^2n-4<0$ implies $c=0$ or $c=\pm1$ and $n=1,2$, or 3. Finally, we can assume $c>0$ by replacing a by $-a$ if necessary.

Definition 30. A polynomial listed in Lemma 29 will be called an *admissible* polynomial.

Remark 31. Lemma 29 shows explicitly that we need consider only finitely many conjugacy classes in the sum (4). Also note that admissible polynomials represent distinct conjugacy classes in Γ (see Lemma 6 of [6]) except that x^2+a and x^2+b with a and $b\|qm$ will represent the same class if and only if a and b differ by a perfect square.

We first calculate the contribution to (4) from $\gamma=1$, i.e. we need

Lemma 32. *$\mathrm{vol}(G/\Gamma)$ is given by $\frac{2}{2^e}M(\mathfrak{O})$ where $M(\mathfrak{O})$ is the mass of $\mathfrak{O}$ and is given by* (2).

Proof. Let $\tilde\gamma_t^{-1}\mathfrak{O}\tilde\gamma_t=\mathfrak{O}_t$, $t=1,\dots,T=T_{qm}$ be a complete set of representatives of the types of orders of level m in $\mathfrak{A}$ and let $U_t=\mathfrak{N}(\mathfrak{O}_t)/J_{\mathbb{Q}}^1$. Then

$$\mathrm{vol}(G/\Gamma)=\sum_{v=1}^{T}\mathrm{vol}(U\tilde\gamma_t\Gamma/\Gamma)=\sum_{v=1}^{T}\mathrm{vol}(U_t\Gamma/\Gamma)$$

$$=\sum_{v=1}^{T}\mathrm{vol}(U_t/U_t\cap\Gamma)=\sum_{v=1}^{T}\frac{1}{|U_t\cap\Gamma|}$$

as $\mathrm{vol}(U)=\mathrm{vol}(U_t)=1$. Let $q_t=|U_t\cap\Gamma|$ and H_t be the class number of two-sided $\mathfrak{O}_t$ ideals (an ideal $\mathfrak{O}_t\tilde a$ is two-sided if $\mathfrak{O}_t\tilde a=\tilde a\mathfrak{O}_t$ and two two-sided $\mathfrak{O}_t$ ideals I and J belong to the same class if $I=Jb$ for some $b\in\mathfrak{A}^*$. Note this forces $b\mathfrak{O}_t=\mathfrak{O}_tb$). We claim $2^e=\frac{2H_tq_t}{w(\mathfrak{O}_t)}$ where recall $w(\mathfrak{O}_t)=|U(\mathfrak{O}_t)|$. By Proposition 10,

$$2^e=[\mathfrak{N}(\mathfrak{O}_t):\mathfrak{U}(\mathfrak{O}_t)J_{\mathbb{Q}}^1]=[\mathfrak{N}(\mathfrak{O}_t):\mathfrak{U}(\mathfrak{O}_t)Q^*].$$

Let T_t be the group of all $\mathfrak{O}_t$ ideals of the form $\mathfrak{O}_ta$, $a\in Q^*$ and let S_t be the group of all two-sided $\mathfrak{O}_t$ ideals. Then the map $\mathfrak{N}(\mathfrak{O}_t)\ni\tilde a\to\mathfrak{O}_t\tilde a$ induces an isomorphism $\mathfrak{N}(\mathfrak{O}_t)/\mathfrak{U}(\mathfrak{O}_t)Q^*\cong S_t/T_t$ and we need only show $[S_t:T_t]=\frac{2H_tq_t}{w(\mathfrak{O}_t)}$. Let P_t be the group of all principal two-sided $\mathfrak{O}_t$ ideals. Then $[S_t:P_t]=H_t$ and it remains to show $[P_t:T_t]=\frac{2q_t}{w(\mathfrak{O}_t)}$. For this consider the surjective homomorphism $U_t\cap\Gamma\to P_t/T_t$ induced by $U_t\cap\Gamma\ni a\to\mathfrak{O}_ta$. Then kernel is $U(\mathfrak{O}_t)Q^*/Q^*\cong U(\mathfrak{O}_t)/(\pm1)$ and the claim is proved. Thus

$$\mathrm{vol}(G/\Gamma)=\sum_{t=1}^{T}\frac{1}{q_t}=\frac{2}{2^e}\sum_{t=1}^{T}\frac{H_t}{w(\mathfrak{O}_t)}$$

and we claim that $M(\mathfrak{O})=\sum_{t=1}^{T}\frac{H_t}{w(\mathfrak{O}_t)}$. But this is almost clear for as in Proposition 8, if $\mathfrak{O}\tilde a_i$, $i=1,\dots,H_{qm}$, represent all $\mathfrak{O}$-ideal classes, then $\tilde a_i^{-1}\mathfrak{O}\tilde a_i$, $i=1,\dots,H_{qm}$, will represent all types of orders of level m in $\mathfrak{A}$ and it is easy to see that exactly H_t of these orders will be of the same type as $\mathfrak{O}_t$ (thus $H_{qm}=\sum_{t=1}^{T_{qm}}H_t$) and as orders of the same type are isomorphic, we are done.

Now we need to consider the contribution $\int_{G/\tilde\Gamma(\gamma)}\varphi_\gamma(x)dx$ to (4) for $\gamma\neq1$. Let $a\in\mathfrak{A}^*$ be a root of some admissible polynomial and suppose $\tilde b=(b_p)\in J_{\mathfrak{A}}^1$ satisfies $\tilde b\tilde a\tilde b^{-1}\in\mathfrak{N}(\mathfrak{O})$. We wish to classify such $\tilde b$. If $p|q$, then $b_pab_p^{-1}\in N(\mathfrak{O}_p)$ for all $b_p\in\mathfrak{A}_p^*$ so there is no restriction on b_p and we have

$$b_pab_p^{-1}\in N(\mathfrak{O}_p)\Leftrightarrow b_pab_p^{-1}\in\mathfrak{O}_p\quad\text{for}\quad p|q. \tag{6}$$

If $p\nmid qm$, then $b_pab_p^{-1}\in N(\mathfrak{O}_p)$ if and only if $b_pab_p^{-1}=u_pc_p$ for some $u_p\in U(\mathfrak{O}_p)$ and $c_p\in Q_p^*$. As $N(a)\in U(Z_p)$, we have

$$b_pab_p^{-1}\in N(\mathfrak{O}_p)\Leftrightarrow b_pab_p^{-1}\in U(\mathfrak{O}_p)\quad\text{for}\quad p\nmid qm. \tag{7}$$

The case $p|m$ is more complicated. If $p|m$, then

$$b_pab_p^{-1}\in N(\mathfrak{O}_p)\Leftrightarrow b_pab_p^{-1}=u_pp^s\pi_p^f \tag{8}$$

where $u_p\in U(\mathfrak{O}_p)$, $s\in Z$, $\pi_p=\begin{pmatrix}0&1\\p^r&0\end{pmatrix}$, $r=v_p(m)$, and $f=0$ or 1 by Proposition 10. If $b_pab_p^{-1}\in N(\mathfrak{O}_p)$, then

$$N(a)=w_pp^{2s}p^{rf}\quad\text{with}\quad w_p\in U(Z_p).$$

Thus we have the following possibilities for (8):

		$v_p(N(a))=0$	$v_p(N(a))=r$
(9)	r odd	$s=f=0$	$s=0,\ f=1$
(10)	r even	$s=f=0$	$s=0,\ f=1$
(10′)		or $s=-r/2,\ f=1$	or $s=r/2,\ f=0$.

Suppose we are in case (10′). Then r is even and a is a root of some x^2+n, $n\geqslant4$. If $v_p(n)=0$, letting $t=r/2$, ap^t is also the root of an admissible polynomial and

$$b_pab_p^{-1}\in\mathfrak{N}(\mathfrak{O})\Leftrightarrow b_pap^tb_p^{-1}\in\mathfrak{N}(\mathfrak{O}).$$

Finally as $b_p a p^t b_p^{-1} = u_p p^{s+t}\pi_p = u_p \pi_p$, we see that case (10′) with $\nu_p(N(a)) = 0$ is equivalent to case (10) with $\nu_p(N(a)) = r$. Similarly case (10′) with $\nu_p(N(a)) = r$ is equivalent to case (10) with $\nu_p(N(a)) = 0$. This leads us to consider $b_p \in \mathfrak{A}_p^*$ with

$$(11) \qquad b_p a b_p^{-1} \in U(\mathfrak{O}_p)\pi_p^f \quad \text{where} \quad f = \begin{cases} 0 & \text{if} \quad \nu_p(N(a)) = 0, \\ 1 & \text{if} \quad \nu_p(N(a)) = r. \end{cases}$$

LEMMA 33. *Let $\gamma \in G$, $\gamma \neq 1$ be such that $\psi_\gamma(x)$ is not identically zero. Let $A(\gamma)$ be a complete set of roots of admissible polynomials (5) in $\mathfrak{A}$, at most one for each polynomial, such that $a \in A(\gamma) \Rightarrow \gamma \equiv a$. For $a \in A(\gamma)$, let*

$$\langle a \rangle = \{\tilde{b} = (b_p) \in J^1_{\mathfrak{A}} \mid b_p \text{ satisfies (6), (7), or (11) depending on whether } p \mid q,\ p \nmid qm,\ \text{or } p \mid m\}.$$

Let $\overline{\langle a \rangle}$ be the image of $\langle a \rangle$ in $G = J^1_{\mathfrak{A}}/J^1_{\mathfrak{Q}}$. Then the support of $\psi_\gamma(x)$ in G consists of the disjoint union of the $\overline{\langle a \rangle}$ over $a \in A(\gamma)$.

Proof. We have shown that the support of $\psi_\gamma(x)$ in $J^1_{\mathfrak{A}}$ consists of the sets $\langle a \rangle$, $a \in A(\gamma)$. It is easy to see that the image $\overline{\langle a \rangle}$ of these sets remains disjoint in G.

We need the following

LEMMA 34. *Let $c = b_p a b_p^{-1} \in \mathfrak{A}_p^*$ be as in (11). Then either $c \in U(\mathfrak{O}_p)$ or $\nu_p(N(c)) = r$, $\nu_p(T(c)) \geqslant r$, and $\nu_p(c_{11}) \geqslant r$ where c_{11} is the $(1,1)$ entry of c. Conversely if $c \in \mathfrak{O}_p$ satisfies either of the above conditions, then $c \in U(\mathfrak{O}_p)\pi_p^f$ with f as in (11).*

Proof. This is trivial.

DEFINITION 35. Let $\gamma \in \Gamma$ with $\gamma \equiv a$ for some $a \in \mathfrak{A}^*$ a root of an admissible polynomial. Let $K = Q(a)$ and let $\mathfrak{o}$ be an order of K containing a. For $p \mid m$ an optimal embedding $\varphi_p\colon \mathfrak{o}_p/K_p \to \mathfrak{O}_p/\mathfrak{A}_p$ is said to be *admissible* if either $\varphi_p(a)$ is a unit of $\mathfrak{O}_p$ or $\nu_p(N(\varphi_p(a))) = r$, $\nu_p(T(\varphi_p(a))) \geqslant r$, and $\nu_p(b_{11}) \geqslant r$ where b_{11} is the $(1,1)$ entry of $\varphi_p(a)$.

Remark 36. Since the a in Definition 35 is the root of an admissible polynomial, for each $p \mid m$ either $\nu_p(N(a)) = 0$ in which case $\varphi_p(a)$ is a unit of $\mathfrak{O}$ or $\nu_p(N(a)) = r$ in which case $\nu_p(N(\varphi_p(a))) = r$ and $\nu_p(T(\varphi_p(a))) \geqslant r$. Thus the only real condition on $\varphi_p(a)$ is the condition on b_{11} when $\nu_p(N(a)) = r$.

LEMMA 37. *Let a be as in Lemma 33 with $K = Q(a)$. Then $\langle a \rangle$ consists of the disjoint union of the double cosets $\mathfrak{N}(\mathfrak{O})\tilde{b}J^1_K$ where $K \cap \tilde{b}^{-1}\mathfrak{O}\tilde{b} = \mathfrak{o}$ for some order $\mathfrak{o}$ of K containing a where $x \to b_p x b_p^{-1}$ induces an admissible optimal embedding of $\mathfrak{o}_p/K_p \to \mathfrak{O}_p/\mathfrak{A}_p$ for all $p \mid m$. Here $\tilde{b} = (b_p)$.* (Compare Lemma 21.)

Proof. First note that if conjugation by b_p induces an admissible optimal embedding, so does conjugation by any element of $N(\mathfrak{O}_p)b_p K_p^*$.

If $\tilde{c} = (c_p) \in \langle a \rangle$, then $a \in K \cap \tilde{c}^{-1}\mathfrak{O}\tilde{c} = \mathfrak{o}$ (say) and by Lemma 34 conjugation by c_p induces an admissible optimal embedding for all $p \mid m$. Conversely, if $a \in \mathfrak{o} = K \cap \tilde{c}^{-1}\mathfrak{O}\tilde{c}$ for some $\tilde{c} \in J^1_{\mathfrak{A}}$ with conjugation by c_p inducing an admissible optimal embedding for $p \mid m$, then $\tilde{c} \in \langle a \rangle$ by Lemma 34.

DEFINITION 38. Let a, K, and $\mathfrak{o}$ be as in Definition 35. Then $D'(\mathfrak{o})$ will be the number of double cosets $\mathfrak{N}(\mathfrak{O})\tilde{b}J^1_K$ satisfying $K \cap \tilde{b}^{-1}\mathfrak{O}\tilde{b} = \mathfrak{o}$ where $x \to b_p x b_p^{-1}$ induces an admissible optimal embedding of $\mathfrak{o}_p/K_p \to \mathfrak{O}_p/\mathfrak{A}_p$ for all $p \mid m$. $D'(\mathfrak{o}_p)$ will denote the local component of $D'(\mathfrak{o})$, i.e. if $p \nmid m$ $D'(\mathfrak{o}_p) = D(\mathfrak{o}_p)$ and if $p \mid m$, $D'(\mathfrak{o}_p)$ is the number of double cosets $N(\mathfrak{O}_p)b_p K_p^*$ satisfying $K_p \cap b_p^{-1}\mathfrak{O}_p b_p = \mathfrak{o}_p$ where $x \to b_p x b_p^{-1}$ induces an admissible optimal embedding of $\mathfrak{o}_p/K_p \to \mathfrak{O}_p/\mathfrak{A}_p$.

Remark 39. It is obvious that $D'(\mathfrak{o}) = \prod_p D'(\mathfrak{o}_p)$. For $p \nmid m$, we have already calculated $D'(\mathfrak{o}_p)$ in § 3. For $p \mid m$, Theorem 13 together with Remark 36 allows us to easily calculate $D'(\mathfrak{o}_p)$.

We need the following

DEFINITION 40. An element $a \in \mathfrak{A}^*$, $a \notin Q^*$ is said to be *pure* if $T(a) = 0$ and *impure* otherwise.

and

LEMMA 41. *Let $\gamma \in \Gamma$.*

(i) *If $\gamma \equiv a$, a impure, then $\Gamma(\gamma) = Q(a)^*/Q^*$.*

(ii) *If $\gamma \equiv a$, a pure, then $[\Gamma(\gamma) : Q^*(a)/Q^*] = 2$.*

Proof. This is easy, see [6], Lemma 9.

By Lemma 37 and Definition 38 we have broken the support of $\psi_\gamma(x)$ in $J^1_{\mathfrak{A}}$ into a number of double cosets $\mathfrak{N}(\mathfrak{O})\tilde{b}J^1_K$ and by Proposition 22 we break these double cosets into the smaller pieces $\mathfrak{U}(\mathfrak{O})\tilde{b}J^1_K$. Thus to evaluate (4), in addition to a lot of counting we need to calculate the volume of the image of $\mathfrak{U}(\mathfrak{O})\tilde{b}J^1_K$ in $G/\Gamma(\gamma)$. By Lemma 41, it suffices to calculate this for $\Gamma(\gamma) = K^*/Q^*$ where $\gamma \equiv a$ and $K = Q(a)$ and we have

LEMMA 42. *Let a, K, $\mathfrak{o}$ be as in Definition 35. Let $\tilde{b} \in J^1_{\mathfrak{A}}$ satisfy*

$$\mathfrak{o} = K \cap \tilde{b}^{-1}\mathfrak{O}\tilde{b} \quad \text{where} \quad x \to b_p x b_p^{-1}$$

induces an admissible optimal embedding of $\mathfrak{o}_p/K_p \to \mathfrak{O}_p/\mathfrak{A}_p$ for all $p \mid m$. Then

$$\operatorname{vol}(\mathfrak{U}(\mathfrak{O})\tilde{b}J^1_K/J^1_Q/K^*/Q^*) = \frac{2}{2^e}\frac{h(\mathfrak{o})}{w(\mathfrak{o})}.$$

Proof (compare Lemma 23 and also [6], Lemma 14). Let

$$J^1_K = \bigcup_{i=1}^{h(\mathfrak{o})} \tilde{x}_i \mathfrak{U}(\mathfrak{o}) K^*.$$

Then

$$\begin{aligned}\operatorname{vol}\big(\mathfrak{U}(\mathfrak{O})\tilde{b}J_K^1/J_Q^1/K^*/Q^*\big) &= h(\mathfrak{o})\operatorname{vol}\big(\mathfrak{U}(\tilde{b}^{-1}\mathfrak{O}\tilde{b})K^*/J_Q^1/K^*J_Q^1/J_Q^1\big)\\ &= h(\mathfrak{o})\operatorname{vol}\big(\mathfrak{U}(\tilde{b}^{-1}\mathfrak{O}\tilde{b})K^*/\mathfrak{U}(Z)K^*\big)\\ &= h(\mathfrak{o})\operatorname{vol}\big(\mathfrak{U}(\tilde{b}^{-1}\mathfrak{O}\tilde{b})/U(\mathfrak{o})/\mathfrak{U}(Z)/U(Z)\big)\\ &= \frac{2h(\mathfrak{o})}{w(\mathfrak{o})}\operatorname{vol}\big(\mathfrak{U}(\tilde{b}^{-1}\mathfrak{O}\tilde{b})/\mathfrak{U}(Z)\big) = \frac{2h(\mathfrak{o})}{w(\mathfrak{o})}\frac{1}{2^e}\end{aligned}$$

as

$$\operatorname{vol}\big(\mathfrak{U}(\tilde{b}^{-1}\mathfrak{O}\tilde{b})/\mathfrak{U}(Z)\big) = \operatorname{vol}\big(\mathfrak{U}(\mathfrak{O})/\mathfrak{U}(Z)\big) = \operatorname{vol}\big(\mathfrak{U}(\mathfrak{O})J_Q^1/J_Q^1\big)$$

which is $1/2^e$ by Proposition 10.

We need two technical results before putting all the pieces together.

LEMMA 43. *Let $\mathfrak{o}$ be an order of $Q(\sqrt{-s})$, s a square free positive integer. Then $w(\mathfrak{o}) = 2$ except in the following two cases: $s = -1$ and $\mathfrak{o} = Z + Z\sqrt{-1}$ in which case $w(\mathfrak{o}) = 4$ or $s = -3$ and $\mathfrak{o} = Z + Z\left(\frac{1+\sqrt{-3}}{2}\right)$ in which case $w(\mathfrak{o}) = 6$.*

Proof. This is trivial.

LEMMA 44. *Let $\mathfrak{o}$ be an order of $K = Q(\sqrt{-s})$, s a square free positive integer. Let $\mathfrak{o}'$ be the maximal order of K and let $f = [\mathfrak{o}' : \mathfrak{o}]$. Then*

$$\frac{h(\mathfrak{o})}{w(\mathfrak{o})} = \frac{h(\mathfrak{o}')}{w(\mathfrak{o}')} f \prod_{p|f}\left(1 - \left(\frac{K}{p}\right)\frac{1}{p}\right).$$

Note that $h(\mathfrak{o}')$ is the class number of K.

Proof.

$$\begin{aligned}h(\mathfrak{o}) = [J_K^1 : \mathfrak{U}(\mathfrak{o})K^*] &= h(\mathfrak{o}')[\mathfrak{U}(\mathfrak{o}')K^* : \mathfrak{U}(\mathfrak{o})K^*]\\ &= h(\mathfrak{o}')[\mathfrak{U}(\mathfrak{o}')/U(\mathfrak{o}') : \mathfrak{U}(\mathfrak{o})/U(\mathfrak{o})].\end{aligned}$$

Thus

$$\frac{h(\mathfrak{o})}{w(\mathfrak{o})} = \frac{h(\mathfrak{o}')}{w(\mathfrak{o}')}[\mathfrak{U}(\mathfrak{o}') : \mathfrak{U}(\mathfrak{o})]$$

and

$$[\mathfrak{U}(\mathfrak{o}') : \mathfrak{U}(\mathfrak{o})] = \prod_p [U(\mathfrak{o}'_p) : U(\mathfrak{o}_p)] = f \prod_{p|f}\left(1 - \left(\frac{K}{p}\right)\frac{1}{p}\right)$$

where

$$\left(\frac{K}{p}\right) = \begin{cases} 1 & \text{if } p \text{ splits in } K,\\ 0 & \text{if } p \text{ ramifies in } K,\\ -1 & \text{if } p \text{ remains prime in } K.\end{cases}$$

Proof of Theorem 26. We need to evaluate (4). The contribution of $\gamma = 1$ to (4) is

$$\int_{G/\Gamma} \psi_1(x)\,dx = \operatorname{vol}(G/\Gamma)$$

which is given by Lemma 32. For $\gamma \neq 1$, by Lemmas 29, 33, 37, Definition 38, Propositions 22, 41 and 42, we must consider for each admissible polynomial belonging to (5) one root say a (if a can be chosen in $\mathfrak{A}^*$) and for each such a, we consider all orders $\mathfrak{o}$ of $Q(a)$ containing a and for each such order calculate

$$g\frac{2}{2^e}D'(\mathfrak{o})E(\mathfrak{o})\frac{h(\mathfrak{o})}{w(\mathfrak{o})} \tag{12}$$

where (by Lemma 41), $g = 1/2$ if a is pure and 1 otherwise. The sum of

$$g\frac{2}{2^e}D'(\mathfrak{o})E(\mathfrak{o})\frac{h(\mathfrak{o})}{w(\mathfrak{o})}$$

over all appropriate orders gives the contribution of all $\gamma \neq 1$ to (4). By Remark 25, no generality is lost in assuming all admissible polynomials have roots in $\mathfrak{A}$. We will use Remark 39 and Proposition 22 to calculate $D'(\mathfrak{o})E(\mathfrak{o})$. Also Lemma 42 will be used without mention.

If a is a root of x^2+1 or x^2+x+1, then $D'(\mathfrak{o}) = D(\mathfrak{o})$ and $D(\mathfrak{o})E(\mathfrak{o})$ has already been calculated in the proof of Theorem 16. Thus the contribution of $\gamma \equiv 1$ or $\gamma \equiv a$ with a a root of x^2+1 or x^2+x+1 is $\frac{1}{2^e}H_{qm}$.

The polynomials x^2+2 and x^2+2x+2 (resp. x^2+3 and x^2+3x+3) occur in (5) only if 2 (resp. 3) $\| qm$. We consider these cases first.

Assume $2 \| qm$. Let $a \in \mathfrak{A}^*$ be a root of x^2+2 (see Remark 25) and let $K = Q(a)$. a generates the maximal order say $\mathfrak{o}$ of K so we consider only $\mathfrak{o}$ and calculate $D'(\mathfrak{o})E(\mathfrak{o})$. If $p \nmid qm$, $D'(\mathfrak{o}_p) = E(\mathfrak{o}_p) = 1$. If $p \mid q$,

$$D'(\mathfrak{o}_p) = 1 \quad \text{and} \quad E(\mathfrak{o}_p) = \left(1 - \left(\frac{-8}{p}\right)\right).$$

If $p \mid m$, $p \neq 2$ it is easy to see

$$D'(\mathfrak{o}_p) = \begin{cases} 1 & \text{if } \left(\frac{-8}{p}\right) = 1,\\ 0 & \text{if } \left(\frac{-8}{p}\right) = -1,\end{cases}$$

and $E(\mathfrak{o}_p) = 2$ if $D'(\mathfrak{o}_p) = 1$. Thus

$$D'(\mathfrak{o}_p)E(\mathfrak{o}_p) = \left(1 + \left(\frac{-8}{p}\right)\right).$$

If $p|m$, $p=2$, we have

$$D'(\mathfrak{o}_p)E(\mathfrak{o}_p)=1=\left(1+\left(\frac{-8}{p}\right)\right).$$

As a is pure, (12) becomes

$$\frac{1}{2^e}\prod_{p|q}\left(1-\left(\frac{-8}{p}\right)\right)\prod_{p|m}\left(1+\left(\frac{-8}{p}\right)\right)\frac{1}{2}.$$

Now let $K=Q(a)$ with a a root of $x^2+2x+2=(x+1)^2+1$. Then a again generates the maximal order, say $\mathfrak{o}$, of K. We have: if $p|q$,

$$D'(\mathfrak{o}_p)E(\mathfrak{o}_p)=\left(1-\left(\frac{-4}{p}\right)\right);$$

if $p|m$, $p\neq 2$,

$$D'(\mathfrak{o}_p)E(\mathfrak{o}_p)=\left(1+\left(\frac{-4}{p}\right)\right);$$

and if $p|m$, $p=2$,

$$D'(\mathfrak{o}_p)E(\mathfrak{o}_p)=1=\left(1+\left(\frac{-4}{2}\right)\right).$$

Thus (12) becomes

$$\frac{2}{2^e}\prod_{p|q}\left(1-\left(\frac{-4}{p}\right)\right)\prod_{p|m}\left(1+\left(\frac{-4}{p}\right)\right)\frac{1}{4}$$

and we have computed the term t_2 of (3).

Now assume $3\|qm$. Let $K=Q(a)$ with a a root of x^2+3. We must consider the non-maximal order $\mathfrak{o}=Z+Z\sqrt{-3}$ and the maximal order $\mathfrak{o}'=Z+Z\left(\frac{1+\sqrt{-3}}{2}\right)$. There are several cases to consider. First note that

$$\frac{h(\mathfrak{o})}{w(\mathfrak{o})}=\frac{1}{2},\qquad \frac{h(\mathfrak{o}')}{w(\mathfrak{o}')}=\frac{1}{6}.$$

Case $2|q$: then $D'(\mathfrak{o}_2)=0\Rightarrow D'(\mathfrak{o})=0$. If $p|q$,

$$D'(\mathfrak{o}'_p)E(\mathfrak{o}'_p)=\left(1-\left(\frac{-3}{p}\right)\right).$$

If $p|m$,

$$D'(\mathfrak{o}'_p)E(\mathfrak{o}'_p)=\left(1+\left(\frac{-3}{p}\right)\right).$$

Case $2|m$: then $D'(\mathfrak{o}'_2)=0$ by Theorem 13 as $[\mathfrak{o}'_2:\mathfrak{o}_2]=2^1$ and x^3+3 has no solution mod 8. If $p|q$,

$$D'(\mathfrak{o}_p)E(\mathfrak{o}_p)=\left(1-\left(\frac{-3}{p}\right)\right).$$

If $p|m$, $p\neq 2$,

$$D'(\mathfrak{o}_p)E(\mathfrak{o}_p)=\left(1+\left(\frac{-3}{p}\right)\right).$$

If $p=2$, then

$D'(\mathfrak{o}_2)E(\mathfrak{o}_2)=2$ if 2 or $4\|m$ and $D'(\mathfrak{o}_2)E(\mathfrak{o}_2)=0$ if $8|m$.

Case $2\nmid qm$: Then $\mathfrak{o}_p=\mathfrak{o}'_p$ for all $p|qm$. Thus

$$D'(\mathfrak{o}_p)E(\mathfrak{o}_p)=D'(\mathfrak{o}'_p)E(\mathfrak{o}'_p)$$

and we have: if $p|q$,

$$D'(\mathfrak{o}_p)E(\mathfrak{o}_p)=\left(1-\left(\frac{-3}{p}\right)\right);$$

if $p|m$, $p\neq 3$,

$$D'(\mathfrak{o}_p)E(\mathfrak{o}_p)=\left(1+\left(\frac{-3}{p}\right)\right)$$

and if $p|m$, $p=3$,

$$D'(\mathfrak{o}_3)E(\mathfrak{o}_3)=1=\left(1+\left(\frac{-3}{3}\right)\right).$$

Still assuming $3\|qm$, let $K=Q(a)$ with a a root of $x^2+3x+3=(x+3/2)^2+3/4$. Then a generates the maximal order $\mathfrak{o}$ of K. If $p|q$,

$$D'(\mathfrak{o}_p)E(\mathfrak{o}_p)=\left(1-\left(\frac{-3}{p}\right)\right).$$

If $p|m$, $p\neq 3$,

$$D'(\mathfrak{o}_p)E(\mathfrak{o}_p)=\left(1+\left(\frac{-3}{p}\right)\right).$$

If $p|m$, $p=3$, $D'(\mathfrak{o}_3)E(\mathfrak{o}_3)=1=\left(1+\left(\frac{-3}{p}\right)\right)$. Thus (12) becomes

$$\frac{2}{2^e}\prod_{p|q}\left(1-\left(\frac{-3}{p}\right)\right)\prod_{p|m}\left(1+\left(\frac{-3}{p}\right)\right)\frac{1}{6}$$

and adding this to the contribution from x^2+3, we get the term t_3 of (3).

We now consider all the other polynomials in (5), i.e. x^2+s, $s \geqslant 4$, $s \| qm$. We write $s = uv^2$ with u square free and $\mathfrak{o} = Z+Z\sqrt{-s}$ and fix this notation for the remainder of this section. We consider two cases.

Case $u = 1$ or $2 \pmod 4$: Let $a = \sqrt{-s} = v\sqrt{-u}$ be a root of x^2+s and suppose as always (by Remark 25) that $a \in \mathfrak{A}$. Then all orders of $K = Q(a)$ which contain a are of the form $Z+Zw\sqrt{-u} = \mathfrak{o}_w$ (say) with $w|v$. We must evaluate $D'(\mathfrak{o}_w)E(\mathfrak{o}_w)$. If $p|q$, $\mathfrak{o}_{wp} = \mathfrak{o}_p$ is maximal and we have

$$D'(\mathfrak{o}_{wp})E(\mathfrak{o}_{wp}) = \left(1-\left(\frac{-4u}{p}\right)\right).$$

If $p|m$, $p\nmid s$, $p \neq 2$, then $\mathfrak{o}_{wp} = \mathfrak{o}_p$ and $N(a) = s$ is a unit mod p and

$$D'(\mathfrak{o}_{wp})E(\mathfrak{o}_{wp}) = \left(1+\left(\frac{-4u}{p}\right)\right).$$

If $2|m$, $2\nmid s$, then $\mathfrak{o}_{w2} = \mathfrak{o}_2$ and letting $2^r \| m$, we have two cases: if $r \geqslant 2$, x^2+s has no solution mod 2^r, so

$$D'(\mathfrak{o}_{w2})E(\mathfrak{o}_{w2}) = 0;$$

if $r = 1$, x^2+s has a unique solution mod 2 and Proposition 22 shows $E(\mathfrak{o}_{w2}) = 1$, so

$$D'(\mathfrak{o}_{w2})E(\mathfrak{o}_{w2}) = \left(1+\left(\frac{-4u}{2}\right)\right).$$

If $p|m$, $p|s$, let $p^r \| m$ (so $p^r \| s$). $\mathfrak{o}_{wp}$ must be of the form $Z_p+Z_p p^t\sqrt{-u}$ for some $t = 0, 1, \ldots, [r/2]$. Then $[\mathfrak{o}_{wp}: \mathfrak{o}_p] = p^\varrho$ for some $\varrho = 0, 1, \ldots, [r/2]$. In order to calculate $D'(\mathfrak{o}_{wp})$ we must by Remark 39 find all solutions mod $p^{r+2\varrho}$ of the simultaneous equations

$$\begin{aligned} x^2+s &\equiv 0 \bmod p^{r+2\varrho}, \\ 2x &\equiv 0 \bmod p^{\varrho}, \\ x &\equiv 0 \bmod p^{r}. \end{aligned} \tag{13}$$

If these have a solution, ϱ must equal zero. Thus only orders $\mathfrak{o}_w$ with $\mathfrak{o}_{wp} = \mathfrak{o}_p$ for all $p|s$ can possibly have $D'(\mathfrak{o}_w) \neq 0$. If $\mathfrak{o}_{wp} = \mathfrak{o}_p$, then $\varrho = 0$ and (13) has a unique solution mod p^r, e.g. $x = 0$. If $D'(\mathfrak{o}_{wp}) \neq 0$, we see easily that $E(\mathfrak{o}_{wp}) = 1$. As $\mathfrak{o}_{wp} = \mathfrak{o}_p$ for all $p\nmid s$, we see $D(\mathfrak{o}_w) = 0$ unless $\mathfrak{o}_w = \mathfrak{o}$ and in that case (12) becomes the term t_s of (3).

Case $u \equiv 3 \pmod 4$: Let $a = \sqrt{-s}$. All orders of $K = Q(a)$ which contain a are of the form $Z+Zw\left(\frac{1+\sqrt{-u}}{2}\right) = \mathfrak{o}_w$ (say) for some $w|2v$.

We must evaluate $D'(\mathfrak{o}_w)E(\mathfrak{o}_w)$. If $p|q$, $p \neq 2$, then $\mathfrak{o}_{wp}$ is maximal, so

$$D'(\mathfrak{o}_{wp})E(\mathfrak{o}_{wp}) = \left(1-\left(\frac{-u}{p}\right)\right).$$

If $2|q$, then $D'(\mathfrak{o}_{w2}) = 1$ if $(w, 2) = 1$ and 0 otherwise. Thus

$$D'(\mathfrak{o}_{w2})E(\mathfrak{o}_{w2}) = \left(1-\left(\frac{-u}{2}\right)\right) \quad \text{if} \quad (w, 2) = 1 \text{ and } 0 \text{ otherwise.}$$

If $p|m$, $p\nmid s$, $p \neq 2$, then $\mathfrak{o}_{wp} = \mathfrak{o}_p$ and $N(a) = s$ is a unit mod p and we have

$$D'(\mathfrak{o}_{wp})E(\mathfrak{o}_{wp}) = \left(1+\left(\frac{-u}{p}\right)\right).$$

If $p|m$, $p|s$, let $p^r \| m$. Then $\mathfrak{o}_{wp}$ must be of the form $Z_p+Z_p p^t\left(\frac{1+\sqrt{-u}}{2}\right)$ for some $t = 0, 1, \ldots, [r/2]$ (or $[r/2]+1$ if $p = 2$). Then $[\mathfrak{o}_{wp}: \mathfrak{o}_p] = p^\varrho$ for some $\varrho = 0, \ldots, [r/2]$ (or $[r/2]+1$ if $p = 2$). In order to calculate $D'(\mathfrak{o}_{wp})$, we must find all solutions mod $p^{r+2\varrho}$ of the simultaneous equations (13). But if these have a solution, ϱ must be zero. Thus only orders $\mathfrak{o}_w$ with $\mathfrak{o}_{wp} = \mathfrak{o}_p$ for all $p|s$, $p|m$ can possibly have $D'(\mathfrak{o}_w) \neq 0$. If $\mathfrak{o}_{wp} = \mathfrak{o}_p$, then (13) has the unique solution $x = 0$ and we see

$D'(\mathfrak{o}_{wp})E(\mathfrak{o}_{wp}) = 1$ if $\mathfrak{o}_{wp} = \mathfrak{o}_p$ for all $p|s$, $p|m$ and is zero otherwise.

Note that we have shown $D'(\mathfrak{o}_w) = 0$ unless $\mathfrak{o}_{wp} = \mathfrak{o}_p$ for all $p \neq 2$. We now consider the prime 2. If $2\nmid qm$, the only orders possibly giving a contribution are $\mathfrak{o}$ and $\mathfrak{o}' = Z+Z\left(\frac{1+\sqrt{-s}}{2}\right)$. Noting that $h(\mathfrak{o}) = h(-s)$ and $h(\mathfrak{o}') = h(-s)/\left(2-(-u/2)\right)$ by Lemma 43, we get the term t_s in this case. If $2|q$, $\mathfrak{o}' = Z+Z\left(\frac{1+\sqrt{-s}}{2}\right)$ is the only order which contributes and we again get the term t_s. If $2|m$, $2|s$, we have already considered this case and only the order $\mathfrak{o}$ can contribute and again we get t_s. Finally we have the case $2|m$, $2\nmid s$. The only orders which can possibly contribute are $\mathfrak{o}$ and $\mathfrak{o}'$. Let $2^r \| m$. Assume $r = 1$. For $D'(\mathfrak{o}_2)$ we consider (by Theorem 13) solutions mod 2 of $x^2+s \equiv 0$ (2). This has the unique (mod 2) solution $x = 1$ and we see $D'(\mathfrak{o}_2) = 1$ and $E(\mathfrak{o}_2) = 2$. For $D'(\mathfrak{o}_2')$, we consider solutions mod 8 of the simultaneous equations $x^2+s \equiv 0$ (mod 8) and $2x \equiv 0$ (mod 2). These have solutions $\Leftrightarrow s = 7\,(8)$ in which case $x = 1, 3, 5, 7$ are all solutions. The inequivalent solutions mod 4 can be taken as $x = 1$, $x = 3$. As $2^{-2\varrho}(-4s)$ is a unit and $1 \equiv -3$ (mod 4), $\varphi_1 \sim \varphi_3$. Thus $D'(\mathfrak{o}_2') = 1$ if $s \equiv 7\,(8)$ and 0 if $s \equiv 3\,(8)$. If $s \equiv 7\,(8)$,

it is easy to see that $E(\mathfrak{o}_2') = 2$. Thus

$$D'(\mathfrak{o}_2)E(\mathfrak{o}_2) = 2 \quad \text{and} \quad D'(\mathfrak{o}_2')E(\mathfrak{o}_2') = \left(1+\left(\frac{-s}{2}\right)\right).$$

This gives the t_s for $2\|m$ and $2\nmid s$. Assume $r = 2$. We find by employing Theorem 13 and Proposition 22 that

$$D'(\mathfrak{o}_2) = \begin{cases} 1 & \text{if} \quad s \equiv 3\ (8) \\ 2 & \text{if} \quad s \equiv 7\ (8) \end{cases} \quad \text{and} \quad E(\mathfrak{o}_2) = 2 \quad \text{in either case.}$$

Thus

$$D'(\mathfrak{o}_2)E(\mathfrak{o}_2) = \left(3+\left(\frac{-s}{2}\right)\right).$$

For $\mathfrak{o}_2'$, we find

$$D'(\mathfrak{o}_2')E(\mathfrak{o}_2') = \left(1+\left(\frac{-s}{2}\right)\right).$$

This gives t_s for $4\|m$ and $2\nmid s$. Assume $r \geqslant 3$. For $D'(\mathfrak{o}_2)$, we consider solutions mod 2^r of $x^2+s \equiv 0 \pmod{2^r}$. Such solutions exist if and only if $s \equiv 7\ (8)$ in which case there are four solutions (mod 2^r), say $\pm\alpha$, $\pm\alpha + 2^{r-1}$. As $-4s$ is not a unit letting $\xi, \xi' \in \{\pm\alpha, \pm\alpha+2^{r-1}\}$,

$$\varphi_\xi \equiv \varphi_{\xi'} \left(\mathrm{mod}\ N(\mathfrak{O}_2)\right) \Leftrightarrow \xi \equiv -\xi' \pmod{2^r} \quad \text{and} \quad \xi^2+s \not\equiv 0 \pmod{2^{r+1}}.$$

It is easy to see that one pair $\{\varphi_\alpha, \varphi_{-\alpha}\}$ or $\{\varphi_{\alpha+2^{r-1}}, \varphi_{-\alpha+2^{r-1}}\}$ of optimal embeddings must be equivalent mod $N(\mathfrak{O}_2)$ and the other pair is not. Thus

$$D'(\mathfrak{o}_2) = \begin{cases} 0 & \text{if} \quad s \equiv 3\ (8), \\ 3 & \text{if} \quad s \equiv 7\ (8). \end{cases}$$

Obviously, $E(\mathfrak{o}_2) = 2$. A similar, though simpler argument shows that

$$D'(\mathfrak{o}_2')E(\mathfrak{o}_2') = \left(1+\left(\frac{-s}{2}\right)\right).$$

This gives the term t_s if $8|m$ and $2\nmid s$ and completes the proof of our Theorem 26.

References

[1] M. Deuring, *Algebren*, New York 1935.

[2] M. Eichler, *Über die Idealklassenzahl total definiter Quaternionen-Algebren*, Math. Zeut. 43 (1937), pp. 102–109.

[3] — *Zur Zahlentheorie der Quaternionen-Algebren*, J. Reine Angew. Math. 195 (1955), pp. 127–151.

[4] M. Eichler, *The Basis Problem for Modular Forms and the Traces of the Hecke Operators, Modular Functions of One Variable I*, Lect. Notes in Math. 320, Springer-Verlag, New York.

[5] H. Hijikata, *Explicit formula of the traces of Hecke operators for* $\Gamma_0(N)$, J. Math. Soc. Japan 26 (1) (1974), pp. 56–82.

[6] A. Pizer, *Type Numbers of Eichler Orders*, J. Reine Angew. Math. 264 (1973), pp. 76–102.

[7] K. Roggenkamp and V. Huber-Dyson, *Lattices over Orders I*, New York 1970.

[8] C. Siegel, *Discontinuous Groups*, Ann. of Math., Second Series 44 (1943), pp. 674–689.

[9] T. Tamagawa, *On Selberg's Trace Formula*, J. Fac. Sci. Univ. Tokyo Sec. I, 8 (1960), pp. 363–380.

[10] — *Harmonic analysis on adele groups*, mimeographed notes taken by L. Goldstein, Advanced Science Seminar on Algebraic Groups, Bowdoin College, Maine 1968.

[11] A. Weil, *Basic Number Theory*, New York 1967.

Received on 17. 2. 1975 (676)