J. Math. Soc. Japan
Vol. 20, Nos. 1-2, 1968

A class number associated with the product of an elliptic curve with itself

To Professor Shôkichi Iyanaga for the congraturation of his 60th birthday

By Tsuyoshi HAYASHIDA

(Received Sept. 12, 1967)
(Revised Dec. 1, 1967)

In a previous paper [3] the existence of curves C on the product variety $E\times E'$ of two elliptic curves E and E' with complex multiplication, with the self-intersection number $(C, C)=2$, was proved. $E\times E'$ is then the Jacobian variety of C, C being a theta divisor on $E\times E'$ (Weil [7], Satz 2). The purpose of this paper is to determine explicitly, in a special case $E=E'$, the number of mutually non-isomorphic such curves C of genus 2. More precisely, we shall determine, for a given elliptic curve E with the ring of endomorphisms isomorphic to the principal order of an imaginary quadratic field $\boldsymbol{Q}(\sqrt{-m})$, the number H of isomorphism classes of canonically polarized Jabobian varieties $(E\times E, C)$, C being a theta divisor, as a function of m. In the case $m\equiv 1 \pmod 4$ and $m>1$, for example, we shall obtain the following result:

$$H=\frac{1}{8}\prod_{p}(p-1)\prod_{p}(p+1)+\frac{1}{4}h-2^{t-4},$$

where the first product extends over all prime factors $p\equiv -1 \pmod 4$ of m, and the second over all prime factors $p\equiv 1 \pmod 4$ of m; and h and t are the class number and the number of distinct prime factors of the discriminant of the principal order of $\boldsymbol{Q}(\sqrt{-m})$, respectively. The determination of the number H is reduced to that of the number of classes and the number of "singular" classes of right ideals of certain (non-maximal) orders of a quaternion algebra, and for this purpose Eichler's method ([1] Satz 10) is applicable.

We denote by $\boldsymbol{Q}$ and $\boldsymbol{Z}$ the field of rational numbers and the ring of rational integers, respectively.

§ 1. Summary from a previous paper.

In this section we shall summarize the parts of our previous paper [3] which relate directly to this paper, and see at the same time how we have been led to a number theoretic problem. Let $Q(\sqrt{-m})$ be an imaginary quadratic number field and $\mathfrak{o}$ its principal order; we take m a square-free positive integer. Let E be a 1-dimensional abelian variety (i.e. an elliptic curve) with the ring $\mathfrak{a}(E)$ of endomorphisms isomorphic to the principal order $\mathfrak{o}$; once for all we identify $\mathfrak{a}(E)$ with $\mathfrak{o}$ through a fixed isomorphism. For any two endomorphisms $\lambda, \mu(\in \mathfrak{o})$ of E, $\{\lambda, \mu\} \neq \{0, 0\}$, the correspondence $h_{\lambda,\mu}: E \ni x \rightarrow (\lambda x, \mu x) \in E\times E$ defines a homomorphism of E into the product $E\times E$ of E with itself. The image of E by $h_{\lambda,\mu}$ is an abelian subvariety of dimension 1 on $E\times E$, namely an elliptic curve lying on $E\times E$; we denote it by $E_{\lambda,\mu}$. Any elliptic curve on $E\times E$ is a translation of some $E_{\lambda,\mu}$. Each endomorphism of $E\times E$ is given by the correspondence: $E\times E \ni (x, y) \rightarrow (px+ry, qx+sy) \in E\times E$, where $p, q, r, s \in \mathfrak{o}$. This endomorphism may be expressed by a matrix $\begin{pmatrix} p & r \\ q & s \end{pmatrix}$. This is an automorphism of $E\times E$ if and only if $ps-qr$ is a unit of $\mathfrak{o}$. The intersection number $(E_{\lambda,\mu}, E_{\xi,\eta})$ of two elliptic curves $E_{\lambda,\mu}$ and $E_{\xi,\eta}$ is given by

$$(1) \qquad (E_{\lambda,\mu}, E_{\xi,\eta}) = \frac{N(\lambda\eta-\mu\xi)}{N(\lambda, \mu)N(\xi, \eta)},$$

where $N(\lambda, \mu)$ denotes the norm of the ideal (λ, μ), etc. Every divisor X on $E\times E$ is algebraically equivalent to a linear combination (with integral coefficients) of elliptic curves; hence basing on the formula (1) we can attach to every divisor X on $E\times E$ a 2 by 2 matrix

$$(2) \qquad M(X) = \begin{pmatrix} k & \alpha \\ \bar{\alpha} & l \end{pmatrix},$$

where k, l are rational integers and $\alpha \in \mathfrak{o}$, and $\bar{\alpha}$ is the complex conjugate of α, such that for any elliptic curve $E_{\lambda,\mu}$,

$$M(E_{\lambda,\mu}) = \frac{1}{N(\lambda, \mu)} \begin{pmatrix} \bar{\mu}\mu & -\bar{\mu}\lambda \\ -\bar{\lambda}\mu & \bar{\lambda}\lambda \end{pmatrix}.$$

For any two rational integers k and l, and any element α of $\mathfrak{o}$, there exists a divisor X on $E\times E$ for which the equality (2) holds. For two divisors X and Y on $E\times E$, $M(X) = M(Y)$ if and only if $X \equiv Y$[1]. The intersection number (X, Y) of two divisors X and Y on $E\times E$ is given by

$$(X, Y) = \det M(X+Y) - \det M(X) - \det M(Y);$$

1) For two divisors X and Y, $X \equiv Y$ means that X is algebraically equivalent to Y.

in particular we have

$$\frac{1}{2}(X, X) = \det M(X).$$

We also have a formula

$$(X, E_{\xi,\eta}) = \frac{1}{N(\xi, \eta)}(\bar{\xi}, \bar{\eta})M(X)\binom{\xi}{\eta}.$$

Now let X be a divisor on $E\times E$ with $(X, X)=2$. Then either X or $-X$ is linearly equivalent to a positive divisor Y ([3], Lemma 4). Let $M(X)$ be given by (2). On account of the relations $kl-\alpha\bar{\alpha}=1$ and $(X, E_{1,0})=k$, we know that the former case occurs if and only if $k>0$. Suppose $E\times E$ is the Jacobian variety of some curve C of genus 2, and Y a theta divisor of it. Then Y is a positive divisor with $(Y, Y)=2$ and Y itself is a curve of genus 2 isomorphic to C. Hence we observe the set of all positive divisors Y on $E\times E$ with $(Y, Y)=2$. The conditions $Y>0$ and $(Y, Y)=2$ mean Y is non-degenerate and $l(Y)=\frac{1}{2}(Y, Y)=1$ (Nishi [6] Th. 6 and Cor.). ($l(Y)$ means the dimension of the complete linear system $|Y|$ determined by Y.) Therefore, if Y and Y' are two positive divisors on $E\times E$ such that $Y\equiv Y'$ and $(Y, Y)=2$, then Y' is a translation of Y. We know that to every matrix $M=\begin{pmatrix} k & \alpha \\ \bar{\alpha} & l\end{pmatrix}$, $k, l\in Z$, $\alpha\in \mathfrak{o}$, $k>0$, $kl-\alpha\bar{\alpha}=1$, there corresponds a positive divisor Y on $E\times E$ with $(Y, Y)=2$ such that $M(Y)=M$; and conversely. And by each such matrix M, Y is determined up to translations. The base of our calculation is the following

LEMMA (Weil [7], Satz 2). *Let A be an abelian variety of dimension 2, and Y be a positive divisor on A such that $(Y, Y)=2$. Then, either Y is irreducible and A is the Jacobian variety of Y, the identity map of Y being the canonical mapping of Y into its Jacobian variety; or Y is a sum of two elliptic curves, $Y=E_1+E_2$, $(E_1, E_2)=1$.*

Now we consider an equivalence relation in the set of all positive divisors Y on $E\times E$, with $(Y, Y)=2$: two such divisors Y and Y' are equivalent to each other if and only if there exists an automorphism Λ of $E\times E$ such that $Y'\equiv \Lambda^{-1}(Y)$. In other words Y and Y' are equivalent to each other if and only if there exists a birational automorphism of $E\times E$ which maps Y onto Y'. We denote by h_1 the number of these equivalence classes (that h_1 is finite was proved in [3], §5; but this will also be established later in §5). If Y is irreducible, then by Weil's lemma, Y is a non-singular curve of genus 2 and $E\times E$ is the Jacobian variety of Y, Y being a theta divisor of $E\times E$; and two such curves are birationally equivalent to each other if and only if they are equivalent in the sense just mentioned above; we denote by H the number of equivalence classes which contain positive irreducible divisors $Y, (Y, Y)=2$.

Finally we denote by h_2 the number of equivalence classes which contain sums of two elliptic curves E_1+E_2, $(E_1, E_2)=2$. Then, by the Lemma we have $H=h_1-h_2$. Suppose an automorphism Λ of $E\times E$ is given by the correspondence: $E\times E\ni(x, y)\rightarrow(px+ry, qx+sy)\in E\times E$, where $p, q, r, s\in\mathfrak{o}$, and $ps-qr$ is a unit of $\mathfrak{o}$. It is easy to see that the condition $Y'\equiv\Lambda^{-1}(Y)$ is written in the following form:

$$M(Y')=\begin{pmatrix}\bar{p} & \bar{q}\\ \bar{r} & \bar{s}\end{pmatrix}M(Y)\begin{pmatrix}p & r\\ q & s\end{pmatrix}.$$

Now we observe the set of all matrices $M=\begin{pmatrix}k & \alpha\\ \bar{\alpha} & l\end{pmatrix}$, where k, l are rational integers, $\alpha\in\mathfrak{o}$, $k>0$ and $\det M=kl-\alpha\bar{\alpha}=1$. We define an equivalence relation in this set: two matrices M and M' are equivalent to each other (notation $M\sim M'$), if and only if there exists a matrix $U=\begin{pmatrix}p & r\\ q & s\end{pmatrix}$, where $p, q, r, s\in\mathfrak{o}$ and $ps-qr$ is a unit of $\mathfrak{o}$, such that $M'={}^t\bar{U}MU$. Then the number of these equivalence classes is equal to h_1.

§ 2. The number h_2.

Two elliptic curves $E_{\alpha,\beta}$ and $E_{\gamma,\delta}$ on $E\times E$ are isomorphic to each other if and only if two ideals (α, β) and (γ, δ) are in the same class ([**3**], Cor. of Prop. 3); and $E_{\alpha,\beta}=E_{\gamma,\delta}$ if and only if $\alpha\delta-\beta\gamma=0$ ([**3**], Cor. 2 of Lemma 3). Suppose two sums of elliptic curves E_1+E_2 and E_3+E_4 with $(E_1, E_2)=(E_3, E_4)=1$ are equivalent. Then there exists a birational automorphism of $E\times E$ which maps E_1+E_2 onto E_3+E_4. Hence E_1 is isomorphic to one of the two elliptic curves E_3 and E_4. The elliptic curve E_1 (resp. E_2) is a translation of an abelian subvariety $E_{\alpha,\beta}$ (resp. $E_{\gamma,\delta}$) of dimension 1 on $E\times E$; and we have $E_1+E_2\equiv E_{\alpha,\beta}+E_{\gamma,\delta}$. What we have just remarked implies that the classes of ideals (α, β) and (γ, δ) are determined by the equivalence classes of the divisor E_1+E_2. Now, since $(E_{\alpha,\beta}, E_{\gamma,\delta})=1$, we have $N(\alpha, \beta)N(\gamma, \delta)=N(\alpha\delta-\beta\gamma)$; and this means $(\alpha, \beta)(\gamma, \delta)=(\alpha\delta-\beta\gamma)$. Hence, if the ideal (α, β) belongs to a class C, say, then the ideal (γ, δ) belongs to the class C^{-1}. There is an isomorphism ι_1 of $E_{\alpha,\beta}\times E_{\gamma,\delta}$ onto $E\times E$ which is the identity map on $E_{\alpha,\beta}$ and on $E_{\gamma,\delta}$ ([**3**], Cor. of Prop. 6). Suppose $E_{\lambda,\mu}+E_{\nu,\kappa}$ is another divisor with $(E_{\lambda,\mu}, E_{\nu,\kappa})=1$, such that $(\lambda, \mu)\in C$, $(\nu, \kappa)\in C^{-1}$. Then there is an isomorphism φ of $E_{\alpha,\beta}\times E_{\gamma,\delta}$ onto $E_{\lambda,\mu}\times E_{\nu,\kappa}$; and an isomorphism ι_2 of $E_{\lambda,\mu}\times E_{\nu,\kappa}$ onto $E\times E$ which is the identity map on $E_{\lambda,\mu}$ and on $E_{\nu,\kappa}$. The composed map $\Lambda=\iota_2\varphi\iota_1^{-1}$ then is an automorphism of $E\times E$ which maps $E_{\alpha,\beta}$ (resp. $E_{\gamma,\delta}$) onto $E_{\lambda,\mu}$ (resp. $E_{\nu,\kappa}$). Hence $E_{\alpha,\beta}+E_{\gamma,\delta}$ is equivalent to $E_{\lambda,\mu}+E_{\nu,\kappa}$. On the other hand, for any elliptic curve $E_{\alpha,\beta}$ on $E\times E$ there exists an elliptic curve $E_{\gamma,\delta}$ such that $(E_{\alpha,\beta}, E_{\gamma,\delta})=1$ ([**3**], Prop. 6). These facts imply that h_2 is equal to the number of pairs $\{C, C^{-1}\}$

of ideal classes. Since the number of classes C for which $C=C^{-1}$, is 2^{t-1}, where t is the number of distinct prime factors of the discriminant of the principal order $\mathfrak{o}$, we have

$$h_2=\frac{1}{2}(h+2^{t-1}),$$

where h is the number of ideal classes of the principal order $\mathfrak{o}$.

§ 3. Quaternion algebra.

In the rest of this paper we shall determine the number h_1. In this section we shall establish a correspondence between the classes of matrices described at the end of § 1 and the classes of right ideals of some orders of a quaternion algebra. We observe a quaternion algebra $K=\boldsymbol{Q}+\boldsymbol{Q}\sqrt{-m}+\boldsymbol{Q}I+\boldsymbol{Q}\sqrt{-m}\,I$, where $I^2=-1$ and $I\sqrt{-m}=-\sqrt{-m}\,I$, over the field $\boldsymbol{Q}$ of rational numbers. By an order in the quaternion algebra K, we understand, as usual, a subring of K, which contains the ring Z of rational integers and is a free $\boldsymbol{Z}$-module of rank 4. If S is a free $\boldsymbol{Z}$-module of rank 4 contained in K, then the set $R=\{\xi\in K\,|\,S\xi\subset S\}$ makes an order in K, which we call the right order of S. For an order R in K, by a right R-ideal we shall mean, in this paper, only such a free $\boldsymbol{Z}$-module S of rank 4 in K, whose right order is equal to R[2]. Now, to every matrix $M=\begin{pmatrix} k & \alpha \\ \bar{\alpha} & l\end{pmatrix}$, $k, l\in Z$, $\alpha\in\mathfrak{o}$, $k>0$, $kl-\alpha\bar{\alpha}=1$, we make correspond a right $\mathfrak{o}$-module

$$A=k\mathfrak{o}+(\alpha+I)\mathfrak{o}$$

in K, where $\mathfrak{o}$ is the principal order of $\boldsymbol{Q}(\sqrt{-m})$. A is then a free $\boldsymbol{Z}$-module of rank 4, and the right order R of A is equal to $\mathfrak{o}+\frac{1}{2}(1+\sqrt{-m}+I)\mathfrak{o}$ if $m\equiv 2$ (mod 4) and $k\equiv l\equiv 0$ (mod 2); R is equal to $\mathfrak{o}+I\mathfrak{o}$ in other cases. To see this, suppose $\lambda+I\mu$ (λ, $\mu\in Q(\sqrt{-m})$) belongs to R. Since $k(\lambda+I\mu)=k(\lambda-\alpha\mu)+(\alpha+I)k\mu$, we have $\lambda'=\lambda-\alpha\mu\in\mathfrak{o}$. Consequently $(\alpha+I)\mu$ $(=-\lambda'+\lambda+I\mu)$ must belong to R. Since for any $\omega\in\mathfrak{o}$ we have $k\omega(\alpha+I)\mu=k(\omega-\bar{\omega})\alpha\mu+(\alpha+I)k\bar{\omega}\mu$ and $(\alpha+I)\omega(\alpha+I)\mu=-kl\bar{\omega}\mu+(\alpha+I)(\omega\alpha+\bar{\omega}\bar{\alpha})\mu$, we see $(\alpha+I)\mu$ belongs to R if and only if $\mu((\omega_0-\bar{\omega}_0)\alpha, k, l, \omega_0\alpha+\bar{\omega}_0\bar{\alpha}, \alpha+\bar{\alpha})\subset\mathfrak{o}$, where $\omega_0=\sqrt{-m}$ if $m\equiv 1$ or 2 (mod 4); $\omega_0=\frac{1}{2}(1+\sqrt{-m})$ if $m\equiv 3$ (mod 4). Since $kl-\alpha\bar{\alpha}=1$, this is equivalent to the condition $\mu(\omega_0-\bar{\omega}_0, k, l, 2)\subset\mathfrak{o}$. Noticing that the congruence

2) For the orders R with which we shall mostly concern in this paper, this definition of right R-ideals proves to be equivalent to that of Eichler (see § 5). His definition is: a right R-ideal is $\bigcap_p \mu_p R(p)\cap K$ where μ_p's are regular elements and $\mu_p R(p)=R(p)$ but for a finite number of primes p.

$\alpha\bar{\alpha}+1\equiv 0 \pmod 4$ is impossible if $m\equiv 1 \pmod 4$, we have the desired result.

We shall say two matrices M and M' are properly equivalent to each other if there exists a matrix U of determinant 1, with elements in $\mathfrak{o}$, such that ${}^t\bar{U}MU=M'$. For two properly equivalent matrices M and M', putting

$$M'=\begin{pmatrix} k' & \alpha' \\ \bar{\alpha}' & l' \end{pmatrix},\quad U=\begin{pmatrix} p & r \\ q & s \end{pmatrix},\quad ps-qr=1,$$

we have the following relation:

$$\begin{pmatrix} \bar{p} & \bar{q} \\ \bar{r} & \bar{s} \end{pmatrix}\begin{pmatrix} k & \alpha+I \\ \bar{\alpha}-I & l \end{pmatrix}\begin{pmatrix} p & r \\ q & s \end{pmatrix}=\begin{pmatrix} k' & \alpha'+I \\ \bar{\alpha}'-I & l' \end{pmatrix}.$$

Since $kl=(\bar{\alpha}-I)(\alpha+I)$, we also have the relation:

$$\rho(k,\alpha+I)\begin{pmatrix} p & r \\ q & s \end{pmatrix}=(k',\alpha'+I). \tag{3}$$

where $\rho=\bar{p}+k^{-1}\bar{q}(\bar{\alpha}-I)$. This means that the two right R-ideals $A=k\mathfrak{o}+(\alpha+I)\mathfrak{o}$ and $A'=k'\mathfrak{o}+(\alpha'+I)\mathfrak{o}$ are in the same class: $\rho A=A'$. Conversely, if two right R- ideals A, A' in the same class are associated with matrices M and M' respectively, we have a relation of the form (3) with $\rho\in K$, $\rho\neq 0$, and $ps-qr$ a unit of $\mathfrak{o}$. Then we have the relation:

$$k\rho\bar{\rho}\begin{pmatrix} \bar{p} & \bar{q} \\ \bar{r} & \bar{s} \end{pmatrix}\begin{pmatrix} k & \alpha+I \\ \bar{\alpha}-I & l \end{pmatrix}\begin{pmatrix} p & r \\ q & s \end{pmatrix}=k'\begin{pmatrix} k' & \alpha'+I \\ \bar{\alpha}'-I & l' \end{pmatrix}.$$

Comparing the coefficients of I, we see that $k\rho\bar{\rho}(ps-qr)=k'$. This means that $ps-qr$ is a positive rational number, and consequently is equal to 1. Hence the two matrices M and M' are properly equivalent.

Now we shall show that if $R=\mathfrak{o}+I\mathfrak{o}$ or $R=\mathfrak{o}+\frac{1}{2}(1+\sqrt{-m}+I)\mathfrak{o}$ (the latter is aamitted only in the case $m\equiv 2 \pmod 4$), then every class of right R-ideals contains a right ideal of the form $A=k\mathfrak{o}+(\alpha+I)\mathfrak{o}$. We begin with

LEMMA 1. *Every right $\mathfrak{o}$-module S contained in K is of the form $\mathfrak{a}+(\gamma+I)\mathfrak{L}$, where $\mathfrak{a}$, $\mathfrak{L}$ are $\mathfrak{o}$-ideals in $\boldsymbol{Q}(\sqrt{-m})$ and γ is an element of $\boldsymbol{Q}(\sqrt{-m})$.*

PROOF. Put $\mathfrak{a}=S\cap\boldsymbol{Q}(\sqrt{-m})$ and $\mathfrak{L}=\{y\mid x,y\in\boldsymbol{Q}(\sqrt{-m}),\ x+Iy\in S\}$. Then $\mathfrak{a}$, $\mathfrak{L}$ are $\mathfrak{o}$-ideals in $\boldsymbol{Q}(\sqrt{-m})$. There exist two elements $\gamma_1+I\beta_1$, $\gamma_2+I\beta_2$ of S such that $(\beta_1,\beta_2)=\mathfrak{L}$. Whenever two elements λ_1, $\lambda_2\in\mathfrak{o}$ satisfy the equation $\beta_1\lambda_1+\beta_2\lambda_2=0$, we have $\gamma_1\lambda_1+\gamma_2\lambda_2\in\mathfrak{a}$. Hence for any element $t\in\mathfrak{L}^{-1}$, we have $(\gamma_1\beta_2-\gamma_2\beta_1)t\in\mathfrak{a}$; and this means $\gamma_1\beta_2-\gamma_2\beta_1\in\mathfrak{a}\mathfrak{L}$. There exist two elements α_1 and α_2 of $\mathfrak{a}$ such that $\gamma_1\beta_2-\gamma_2\beta_1=\alpha_2\beta_1-\alpha_1\beta_2$, so that $(\gamma_1+\alpha_1)\beta_2-(\gamma_2+\alpha_2)\beta_1=0$. Since γ_1 (resp. γ_2) may be replaced by $\gamma_1+\alpha_1$ (resp. $\gamma_2+\alpha_2$), the proof is completed.

LEMMA 2. *Let $S\subset K$ be a right $\mathfrak{o}$-module and a free $\boldsymbol{Z}$-module of rank 4. Then there exists an element $\rho\neq 0$ of K such that $\rho S\cap\boldsymbol{Q}(\sqrt{-m})=\mathfrak{o}$.*

PROOF. We write S in the form stated in Lemma 1: $S=\mathfrak{a}+(\gamma+I)\mathfrak{L}$. If $\rho_1=\lambda+I\mu$ is an element of K, then $\rho_1 S=\mathfrak{a}_1+(\gamma_1+I)\mathfrak{L}_1$, with $\mathfrak{L}_1=(\mu\mathfrak{a}, (\mu\gamma+\bar{\lambda})\mathfrak{L})$. Since S is a free $\boldsymbol{Z}$-module of rank 4, we have $\mathfrak{a}\neq 0$, $\mathfrak{L}\neq 0$. Hence we can find two elements λ', μ' of $\boldsymbol{Q}(\sqrt{-m})$ such that $(\mu'\mathfrak{a}, \lambda'\mathfrak{L})=\mathfrak{o}$. Taking $\lambda=\bar{\lambda}'-\bar{\mu}'\bar{\gamma}$, $\mu=\mu'$, we have $\rho_1 S=\mathfrak{a}_1+(\gamma_1+I)\mathfrak{o}$, say. Then $\rho=(\gamma_1+I)^{-1}\rho_1$ has the desired property.

LEMMA 3. *A right* $\mathfrak{o}$-*module* $S=\mathfrak{o}+(\gamma+I)\mathfrak{L}$ *is a right* $\mathfrak{o}+I\mathfrak{o}$-*module if and only if* $\mathfrak{L}\neq 0$, $\mathfrak{L}^{-1}\subset\mathfrak{o}$, $\mathfrak{L}=\bar{\mathfrak{L}}$, $\gamma\in\mathfrak{o}$, *and* $\gamma\bar{\gamma}+1\in\mathfrak{L}^{-1}$.

PROOF. For any element $\omega\in\mathfrak{o}$, we have $\omega I=-\gamma\bar{\omega}+(\gamma+I)\bar{\omega}$; and for any element $\beta\in\mathfrak{L}$, $(\gamma+I)\beta I=-(1+\gamma\bar{\gamma})\bar{\beta}+(\gamma+I)\bar{\gamma}\bar{\beta}$. Hence $SI\subset S$ if and only if $\gamma\in\mathfrak{o}$, $\mathfrak{o}\subset\mathfrak{L}$, $(1+\gamma\bar{\gamma})\bar{\mathfrak{L}}\subset\mathfrak{o}$, and $\bar{\gamma}\bar{\mathfrak{L}}\subset\mathfrak{L}$. These relations imply $\gamma\bar{\gamma}\bar{\mathfrak{L}}\subset\mathfrak{L}$ and $(1+\gamma\bar{\gamma})\bar{\mathfrak{L}}\subset\mathfrak{L}$, so that $\bar{\mathfrak{L}}\subset\mathfrak{L}$; consequently $\bar{\mathfrak{L}}=\mathfrak{L}$. Thus we see the conditions stated in this Lemma are necessary. Sufficiency is obvious.

Let $S=\mathfrak{o}+(\gamma+I)\mathfrak{L}$ be a right $\mathfrak{o}+I\mathfrak{o}$-module in K. By Lemma 3 we can put $\mathfrak{L}^{-1}=k\mathfrak{a}_0$ and $\gamma\bar{\gamma}+1=kla_0$, where k, l are positive rational integers; $\mathfrak{a}_0$ is primitive ambiguous ideal in $\mathfrak{o}$, and a_0 is the norm of $\mathfrak{a}_0$: $\mathfrak{a}_0=a_0\boldsymbol{Z}+(r+\omega_0)\boldsymbol{Z}$ with $r\in\boldsymbol{Z}$. The right order of S is given by

LEMMA 4. *The notation being as above, the right order* $R=\{\xi\mid\xi\in K, S\xi\subset S\}$ *of a right* $\mathfrak{o}+I\mathfrak{o}$-*module* S *is equal to* $\mathfrak{o}+\frac{1}{2}(\gamma+I)\mathfrak{a}_0^{-1}$ *if* $m\equiv 2 \pmod 4$ *and* $k\equiv l\equiv 0 \pmod 2$; $\mathfrak{o}+(\gamma+I)\mathfrak{a}_0^{-1}$ *otherwise*.

PROOF. Suppose $\xi=x+(\gamma+I)y$ with $x, y\in\boldsymbol{Q}(\sqrt{-m})$ is an element of R. Since $1\in S$, we have $\xi\in S$; and consequently $x\in\mathfrak{o}$ and $(\gamma+I)y\in R$. Therefore R is of the form $\mathfrak{o}+(\gamma+I)\mathfrak{C}$, where $\mathfrak{C}$ is an $\mathfrak{o}$-ideal in $\boldsymbol{Q}(\sqrt{-m})$. For any element $\omega\in\mathfrak{o}$ we have $\omega(\gamma+I)=(\omega-\bar{\omega})\gamma+(\gamma+I)\bar{\omega}$; and for any element $\beta\in k^{-1}\mathfrak{a}_0^{-1}$ we have $(\gamma+I)\beta(\gamma+I)=-(\gamma\bar{\gamma}+1)\bar{\beta}+(\gamma+I)(\beta\gamma+\bar{\beta}\bar{\gamma})$. Then $\mathfrak{C}$ is the greatest subset of $\boldsymbol{Q}(\sqrt{-m})$ satisfying the relations: $(\omega_0-\bar{\omega}_0)\gamma\mathfrak{C}\subset\mathfrak{o}$, $\mathfrak{C}\subset k^{-1}\mathfrak{a}_0^{-1}$, $(\gamma\bar{\gamma}+1)k^{-1}\mathfrak{a}_0^{-1}\mathfrak{C}\subset\mathfrak{o}$, $T_r(k^{-1}\mathfrak{a}_0^{-1}\gamma)\mathfrak{C}\subset k^{-1}\mathfrak{a}_0^{-1}$. Hence we have an equality $\mathfrak{C}^{-1}=((\omega_0-\bar{\omega}_0)\gamma, k\mathfrak{a}_0, l\mathfrak{a}_0, \mathfrak{a}_0 T_r(\mathfrak{a}_0^{-1}\gamma))$. Now we know $\gamma\in\mathfrak{o}$ (Lemma 3), and $\mathfrak{C}^{-1}\subset\mathfrak{o}$. The relation $\gamma\bar{\gamma}+1=kla_0$ implies γ is relatively prime to $\mathfrak{C}^{-1}$. Hence we have $\omega_0-\bar{\omega}_0\in\mathfrak{C}^{-1}$. For any two elements $\alpha, \alpha'\in\mathfrak{a}_0$ we have a congruence $\alpha'(\alpha\gamma+\bar{\alpha}\bar{\gamma})a_0^{-1}\equiv(\alpha'+\bar{\alpha}')\alpha\gamma a_0^{-1} \pmod{\mathfrak{C}^{-1}}$. Thus from the above equality we have a formula $\mathfrak{C}^{-1}=(\omega_0-\bar{\omega}_0, k\mathfrak{a}_0, l\mathfrak{a}_0, \mathfrak{a}_0 T_r(\mathfrak{a}_0^{-1}))$. Now, if $m\equiv 3 \pmod 4$, then $\omega_0-\bar{\omega}_0=\sqrt{-m}\in\mathfrak{a}_0$ and $T_r(\mathfrak{a}_0^{-1})=(1)$. Hence by this formula $\mathfrak{C}^{-1}=\mathfrak{a}_0$. If $m\equiv 1 \pmod 4$, then $\omega_0-\bar{\omega}_0=2\sqrt{-m}\in\mathfrak{a}_0$ and $T_r(\mathfrak{a}_0^{-1})=(1)$ or (2); and, since the congruence $\gamma\bar{\gamma}+1\equiv 0 \pmod 4$ is impossible, we have $(k, l, 2)=1$. Hence $\mathfrak{C}^{-1}=\mathfrak{a}_0$. If $m\equiv 2 \pmod 4$, then $\omega_0-\bar{\omega}_0=2\sqrt{-m}\in 2\mathfrak{a}_0$ and $T_r(\mathfrak{a}_0^{-1})=(2)$. Hence we have $\mathfrak{C}^{-1}=(k, l, 2)\mathfrak{a}_0$. This settles our assertion.

Now suppose S be a free $\boldsymbol{Z}$-module of rank 4 contained in K, whose right order is $\mathfrak{o}+I\mathfrak{o}$ or $\mathfrak{o}+\frac{1}{2}(1+\sqrt{-m}+I)\mathfrak{o}$ (the latter is admitted only in the case $m\equiv 2 \pmod 4$). Since $\mathfrak{o}+I\mathfrak{o}\subset\mathfrak{o}+\frac{1}{2}(1+\sqrt{-m}+I)\mathfrak{o}$, S is in any case a right $\mathfrak{o}+I\mathfrak{o}$-module and Lemma 1-4 are applicable to S. By Lemmas 2 and 3 there exists a regular element $\rho\in K$ such that ρS is of the form $\mathfrak{o}+(\gamma+I)k^{-1}\mathfrak{a}_0^{-1}$; and by Lemma 4 the right order of S is equal to $\mathfrak{o}+(\gamma+I)\mathfrak{a}_0^{-1}$ or $\mathfrak{o}+\frac{1}{2}(\gamma+I)\mathfrak{a}_0^{-1}$ (the latter is possible only if $m=2 \pmod 4$). It is easy to see that if the right order of S is $\mathfrak{o}+I\mathfrak{o}$, then the former holds; if $\mathfrak{o}+\frac{1}{2}(1+\sqrt{-m}+I)\mathfrak{o}$, then the latter. In either case we have $\mathfrak{a}_0=\mathfrak{o}$. (Notice that since $\mathfrak{a}_0$ is an primitive integral ideal of $\mathfrak{o}$, $\mathfrak{a}_0$ can not be equal to $\frac{1}{2}\mathfrak{o}$ or $2\mathfrak{o}$.) Thus, for an order $R=\mathfrak{o}+I\mathfrak{o}$ or $\mathfrak{o}+\frac{1}{2}(1+\sqrt{-m}+I)\mathfrak{o}$, every class of right R-ideals contains an ideal of the form $A=k\rho S=k\mathfrak{o}+(\gamma+I)\mathfrak{o}$. Therefore there is a one-to-one correspondence between proper classes of matrices M described above and classes of right R-ideals ($R=\mathfrak{o}+I\mathfrak{o}$ or $\mathfrak{o}+\frac{1}{2}(1+\sqrt{-m}+I)\mathfrak{o}$). If $m\neq 1$ or 3, the principal order $\mathfrak{o}$ of $\boldsymbol{Q}(\sqrt{-m})$ contains only two units, namely ± 1; hence one class of matrices M consists of one or two proper classes. In the former case, in this paper, the class of matrices M or the corresponding right R-ideals will be called singular. We denote by H' the number of proper classes of matrices M, where $M=\begin{pmatrix} k & \alpha \\ \bar{\alpha} & l\end{pmatrix}$, $k, l\in\boldsymbol{Z}$, $\alpha\in\mathfrak{o}$, $k>0$, $kl-\alpha\bar{\alpha}=1$; and by H'' the number of singular classes of matrices M. We have then $h_1=\frac{1}{2}(H'+H'')$ $(m\neq 1, 3)$. Also we denote by $H'(R)$ (resp. $H''(R)$) the number of classes (resp. singular classes) of right R-ideals. In the case $m\not\equiv 2 \pmod 4$ we have $H'=H'(R)$, $H''=H''(R)$ where $R=\mathfrak{o}+I\mathfrak{o}$; and in the case $m\equiv 2 \pmod 4$ we have $H'=\sum_R H'(R)$, $H''=\sum_R H''(R)$ where the sums extend over two orders $R=\mathfrak{o}+I\mathfrak{o}$ and $R=\mathfrak{o}+\frac{1}{2}(1+\sqrt{-m}+I)\mathfrak{o}$.

§ 4. p-adic extension.

Let $\boldsymbol{Q}(p)$ be the field of p-adic numbers and $\boldsymbol{Z}(p)$ the ring of p-adic integers. We denote by $R(p)$ (resp. $A(p)$) the p-adic extension of an order R (resp. an ideal A): $R(p)=R\otimes_{\boldsymbol{Z}}\boldsymbol{Z}(p)$ (resp. $A(p)=A\otimes_{\boldsymbol{Z}}\boldsymbol{Z}(p)$). Also we put $K(p)=K\otimes_{\boldsymbol{Q}}\boldsymbol{Q}(p)$. If R is an order in the quaternion algebra K, then $R(p)$ is an order in $K(p)$, i.e. a subring of $K(p)$, which contains $\boldsymbol{Z}(p)$ and is a free $\boldsymbol{Z}(p)$-module of rank 4. We shall understand, in this paper, by a right $R(p)$-ideal a free $\boldsymbol{Z}(p)$-module of rank 4 in $K(p)$, whose right order is equal to $R(p)$. We can easily see that if A is a right R-ideal, then $A(p)$ is a right $R(p)$-ideal. Let $[\lambda_1, \lambda_2, \lambda_3, \lambda_4]$ be a $\boldsymbol{Z}$-basis of an order R in K. By the discriminant of R we understand $D=\det(T_r(\bar{\lambda}_i\lambda_j))$, where $\bar{\lambda}_i$ means the conjugate of λ_i in the quaternion algebra K. By the level of an order R we understand the positive rational integer

$$q=n(\tilde{R})^{-1}$$

where $\tilde{R}$ means the complementary ideal of R and $n(\tilde{R})$ the greatest common divisor of the norms of elements of $\tilde{R}$. (The comlpementary ideal $\tilde{R}$ of R is one which has a $\boldsymbol{Z}$-basis $[\mu_1, \mu_2, \mu_3, \mu_4]$ such that $T_r(\bar{\lambda}_i\mu_j)=1$ if $i=j$; $=0$ if $i\neq j$.) The p-component of D (resp. q) is equal to the discriminant (resp. the level) of the p-adic extension $R(p)$. It is known that if $p\,\|\,q$ (i. e. $q\equiv 0 \pmod p$ and $q\not\equiv 0 \pmod{p^2}$), then $p^2\,\|\,D$ ([1] § 2). For the orders $R=\mathfrak{o}+I\mathfrak{o}$ and $R=\mathfrak{o}+\frac{1}{2}(1+\sqrt{-m}+I)\mathfrak{o}$ (the latter is admitted only in the case $m\equiv 2 \pmod 4$), by a simple calculation we know that $q=m$ if a) $m\equiv 3 \pmod 4$, or b) $m\equiv 2 \pmod 4$ and $R=\mathfrak{o}+\frac{1}{2}(1+\sqrt{-m}+I)\mathfrak{o}$; and that $q=4m$ if c) $m\equiv 1 \pmod 4$, or d) $m\equiv 2 \pmod 4$ and $R=\mathfrak{o}+I\mathfrak{o}$. And $D=q^2$ (though the prime $p=2$ does not satisfy the above condition). It is known that if $K(p)=K\otimes_{\boldsymbol{Q}}\boldsymbol{Q}(p)$ is a division algebra, then $p\,|\,q$. We denote by q_1 the product of all and different such primes p. By a simple calculation we know that an odd prime factor p of q divides q_1 if and only if $p\equiv 3 \pmod 4$; and $2\,|\,q_1$ if and only if $m\equiv 1 \pmod 4$ or $m\equiv 2 \pmod 8$. We put $q=q_1q_2$. Now let p be an odd prime and $p\,|\,q_1$. Since we have $p\,\|\,q$ by the above result, $R(p)$ is the (unique) maximal order of the division algebra $K(p)$; and every right ideal of $R(p)$ is two-sided and principal, and is a power of the unique prime ideal $\pi R(p)$ where π is a prime element in $R(p)$. Next let p be an odd prime, $p\,|\,q_2$. Then we have $p\,\|\,q$ by the above result, and we know ([1] § 2) that $R(p)$ is isomorphic to an order of 2 by 2 matrices with components in $\boldsymbol{Z}(p)$, the left-lower component being divisible by p:

$$R(p)\cong\begin{pmatrix}\boldsymbol{Z}(p) & \boldsymbol{Z}(p)\\ p\boldsymbol{Z}(p) & \boldsymbol{Z}(p)\end{pmatrix}.$$

We shall show that every right $R(p)$-ideal $A(p)$ is of the form $A(p)=\mu R(p)$ with μ a regular element in $K(p)$. Represent all elements of $R(p)$ by 2 by 2 matrices through the above isomorphism. It is easy to see that the set of the first rows of all elements of $A(p)$ then make a left $R(p)$-module of the form either $(p^a\boldsymbol{Z}(p), p^a\boldsymbol{Z}(p))$ or $(p^{a+1}\boldsymbol{Z}(p), p^a\boldsymbol{Z}(p))$. The former is generated by $(p^a, 0)$; and the latter by $(0, p^a)$. Similarly, the set of the second rows of those elements of $A(p)$, of which the first rows are zeros, makes a left $R(p)$-module generated by either $(p^b, 0)$ or $(0, p^b)$. And $A(p)$ is the direct sum of these two type of left $R(p)$-modules. Among the 4 possible combinations, however, the former-former one or the latter-latter one gives a maximal order (instead of $R(p)$) as the right order. The former-latter one or the latter-former one gives $R(p)$ as the right order; and $A(p)$ then is equal to $\mu R(p)$ where

$$\mu=\begin{pmatrix} p^a & 0 \\ c & p^b \end{pmatrix},\ c \bmod p^{b+1}, \text{ or } \mu=\begin{pmatrix} 0 & p^a \\ p^b & c \end{pmatrix},\ c \bmod p^b,$$

respectively. Therefore in this case our definition of right $R(p)$-ideals is equivalent to that of Eichler. We know that every two-sided ideal of $R(p)$ is a power of the two-sided ideal $\pi R(p)$, where $\pi=\begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}$ ([1] § 2). Remark that the ideal $\pi R(p)$ is invariant under the canonical involution of $K(p)$ (i.e. equal to its conjugate). Next let p be a prime, $p \nmid q$. Then $R(p)$ is a maximal order in $K(p)$, isomorphic to the order of all 2 by 2 matrices with components in $\boldsymbol{Z}(p)$. We can see in like manner that our definition of right-ideals is equivalent to that of Eichler; and every right $R(p)$-ideal is uniquely written in the form

$$\begin{pmatrix} p^a & 0 \\ c & p^b \end{pmatrix} R(p),\ c \bmod p^b.$$

Every two-sided $R(p)$-ideal is of the form $p^a R(p)$. Finally let $p=2$. We shall prove the following

LEMMA 5. *Every right $R(2)$-ideal is equal to a principal ideal $\mu R(2)$ with a regular element μ in $K(2)$.*

PROOF. In the case a) $m\equiv 3 \pmod 4$, we have $p=2\nmid q$ and hence the Lemma is true. In the case b) $m\equiv 2 \pmod 4$ and $R=\mathfrak{o}+\frac{1}{2}(1+\sqrt{-m}+I)\mathfrak{o}$ we have $p=2 \| q$ $(q=m)$; then we can prove the Lemma in the same way as in the case of odd p, $p\| q$. We shall treat the case c) $m\equiv 1 \pmod 4$ and the case d) $m\equiv 2 \pmod 4$ and $R=\mathfrak{o}+I\mathfrak{o}$. In either case the order R is equal to $\mathfrak{o}+I\mathfrak{o}$ and the rational prime 2 ramifies in $\mathfrak{o}$. Suppose S is a right $R(2)$-ideal. We denote by $\mathfrak{o}(2)$ the 2-adic extension of the principal order $\mathfrak{o}$ of $\boldsymbol{Q}(\sqrt{-m})$. Since S is a right $\mathfrak{o}(2)+I\mathfrak{o}(2)$-module in $K(2)$ and a free $\boldsymbol{Z}(2)$-module of rank 4, and since every ideal of $\mathfrak{o}(2)$ is a power of the prime ideal $\pi\mathfrak{o}(2)$ where π is a prime element in $\mathfrak{o}(2)$, we can put $S=\pi^t(\mathfrak{o}(2)+(\gamma+I)\pi^{-s}\mathfrak{o}(2))$, $\gamma\in\boldsymbol{Q}(2)(\sqrt{-m})$. The conditions $SI\subset S$ means, as in Lemma 3, that $\gamma\in\mathfrak{o}(2)$, $s\geqq 0$, and $\pi^s|\gamma\bar{\gamma}+1$. Then we see, as in the proof of Lemma 4, that the right order of S is of the form $\mathfrak{o}(2)+(\gamma+I)\pi^{-u}\mathfrak{o}(2)$ and the ideal $\pi^{-u}\mathfrak{o}(2)$ is determined by the equality $\pi^u\mathfrak{o}(2)=((\omega_0-\bar{\omega}_0)\gamma,\ (\gamma\bar{\gamma}+1)\pi^{-s},\ \pi^s,\ \pi^s T_r(\pi^{-s}\gamma\mathfrak{o}(2)))$. Since, by our assumption, the right order of S is $R(2)=\mathfrak{o}(2)+I\mathfrak{o}(2)$, u ought to be 0. Since $2|\omega_0-\bar{\omega}_0(=2\sqrt{-m})$ and $\pi^s T_r(\pi^{-s}\gamma\mathfrak{o}(2))\subset\pi\mathfrak{o}(2)$, this means that π^s or $(\gamma\bar{\gamma}+1)\pi^{-s}$ is a unit of $\mathfrak{o}(2)$. In the former case we have $S=\pi^t R(2)$; and in the latter case we have $S=\pi^t(\bar{\gamma}-I)^{-1}R(2)$.

Hence our assertion is proved.

By Lemma 5 we know that, also for the prime $p=2$, our definition of right $R(2)$-ideals is equivalent to that of Eichler. Next we shall determine the two-sided $R(2)$-ideals and the number of integral right $R(2)$-ideals with given norm. At the end of our proof of Lemma 5, we have seen that, in the case c) or d), every right $R(2)$-ideal is written in the form $\pi^t R(2)$ or $\pi^t(\bar{\gamma}-I)^{-1}R(2)$ where $\gamma\in\mathfrak{o}(2)$ and π is a prime element of $\mathfrak{o}(2)$. First in the case c), if $\bar{\gamma}-I$ is not a unit of $R(2)$, then, putting $\gamma=a+b\sqrt{-m}$, $a, b\in \boldsymbol{Z}(2)$, one of the two elements a and b is odd and the other is even; hence $(1+I)(\bar{\gamma}-I)^{-1}$ or $(\sqrt{-m}+I)(\bar{\gamma}-I)^{-1}$ is a unit of $R(2)$. We can see that three right $R(2)$-ideals $A=\pi R(2)=(1+\sqrt{-m})R(2)$, $B=(1+I)R(2)$, $C=(\sqrt{-m}+I)R(2)$ are two-sided[3] and satisfy the following relations: $A^2=B^2=C^2=2R(2)$, $AB=BC=CA$ and $BA=CB=AC$. Consequently we know that every right $R(2)$-ideal is two-sided and can be written uniquely in one of the three forms: A^n, A^nB, A^nC. Remark that the ideals A, B, C are invariant under the canonical involution of $K(2)$, respectively; the ideal AB is (two-sided and yet) not invariant under the canonical involution. Now we consider the case d) $m\equiv 2 \pmod 4$ and $R=\mathfrak{o}+I\mathfrak{o}$. It is easy to see that the two right ideals $A=\sqrt{-m}R(2)$ and $B=(1+I)R(2)$ are two-sided and satisfy the relations: $A^2=B^2=2R(2)$, $AB=BA$. Let $S=\alpha R(2)$, where $\alpha=a+bI+c\sqrt{-m}+d\sqrt{-m}I\in R(2)$, be an integral right $R(2)$-ideal. If $a\not\equiv b \pmod 2$, then α is a unit of $R(2)$ and $S=R(2)$. If $a\equiv b\equiv 0 \pmod 2$, then α is factorized as follows: $\alpha=\alpha'\sqrt{-m}$, $\alpha'\in R(2)$. If $a\equiv b\equiv 1 \pmod 2$ and $c\equiv d \pmod 2$, then α is factorized as follows: $\alpha=\alpha'(1+I)$, $\alpha'\in R(2)$. In what follows, those elements $\alpha=a+bI+c\sqrt{-m}+d\sqrt{-m}I$ of $R(2)$ which satisfy the condition: $a\equiv b\equiv 1 \pmod 2$, $c\not\equiv d \pmod 2$, will be called primitive. If $\alpha\in R(2)$ is primitive, then $c+dI$ is a unit of $R(2)$ and $\alpha'=\alpha(c+dI)^{-1}$ is also primitive and has the form $\alpha'=a'+b'I+\sqrt{-m}$. Suppose $\alpha=a+bI+\sqrt{-m}$ and $\alpha'=a'+b'I+\sqrt{-m}$ are two primitive elements of $R(2)$ and α is not a zero-divisor and $2^s\,\|\,\bar{\alpha}\alpha$. Since $\bar{\alpha}\alpha'=(a-bI-\sqrt{-m})(a'+b'I+\sqrt{-m})=aa'+bb'+m+(ab'-ba')I+(a-a')\sqrt{-m}+(b-b')\sqrt{-m}I$, $\alpha'\in\alpha R(2)$ if and only if $a\equiv a'$, $b\equiv b' \pmod{2^s}$. And the last congruences imply $a^2+b^2+m\equiv a'^2+b'^2+m \pmod{2^{s+1}}$; consequently $\alpha'=\alpha\varepsilon$, where ε is a unit of $R(2)$. Hence we have $\alpha R(2)=\alpha' R(2)$ if and only if $a\equiv a'$, $b\equiv b' \pmod{2^s}$. On the other hand, if $\alpha=a+bI+\sqrt{-m}$ is any primitive element of $R(2)$, then $\alpha''=\alpha\sqrt{-m}(1+I)^{-1}=-\frac{1}{2}m+\frac{1}{2}mI+\frac{1}{2}(a-b)\sqrt{-m}-\frac{1}{2}(a+b)\sqrt{-m}I$ is also a primitive element of $R(2)$; and we

3) In fact $R(2)$ is the unique order of level 4 in $K(2)$, in this case. But this is not necessary in what follows.

have $\alpha\sqrt{-m}R(2)=\alpha''(1+I)R(2)$. An integral ideal $\alpha R(2)$, $\alpha\in R(2)$, will be called primitive if α is primitive and is not a zero-divisor. Since the product of a primitive element and a unit of $R(2)$ is also primitive, the definition of a primitive ideal is independent of the choice of α. Now, in the case $m\equiv 2 \pmod 8$, for any primitive element $\alpha=a+bI+\sqrt{-m}$ we have $\alpha\bar{\alpha}=a^2+b^2+m\equiv 4$ (mod 8). Hence, corresponding to 4 primitive elements $\alpha=\pm 1\pm I+\sqrt{-m}$ there exist just 4 primitive ideals C_i $(i=1, 2, 3, 4)$, say, with norm 4. And every integral right $R(2)$-ideal is uniquely expressible in one of the forms: A^n, BA^n, C_iA^n $(1\leqq i\leqq 4;\ n=0, 1, 2, \cdots)$. In the case $m\equiv 6 \pmod 8$, for any integer $s\geqq 3$, the congruence $x^2+y^2+m\equiv 2^s \pmod{2^{s+1}}$ has 2^s solutions $x, y \pmod{2^s}$ (notice that, for any element $a\in \boldsymbol{Z}(2)$, $a\equiv 1 \pmod 8$, the congruence $x^2\equiv a \pmod{2^{s+1}}$ has just 2 solutions x mod 2^s); and corresponding to the 2^s primitive elements $x+yI+\sqrt{-m}$ there exist just 2^s primitive ideals with norm 2^s. Denoting by C_i $(i=1, 2, 3, \cdots)$ all the primitive ideals of $R(2)$, every integral right $R(2)$-ideal is uniquely expressible in one of the forms: A^n, BA^n, C_iA^n $(i=1, 2, 3, \cdots;\ n=0, 1, 2, \cdots)$. Finally, in the case $m\equiv 2$ or $6 \pmod 8$, we determine the two-sided ideals of $R(2)$. For any primitive element $\alpha=a+bI+\sqrt{-m}\in R(2)$ which is not a zero-divisor, $\alpha I\bar{\alpha}$ is not divisible by 4 (because, putting $\alpha I\bar{\alpha}=a'+b'I+c'\sqrt{-m}+d'\sqrt{-m}I$, we have $c'=2b$), so that $\alpha R(2)\bar{\alpha}\not\subset R(2)\alpha\bar{\alpha}$, i.e. $\alpha R(2)\not\subset R(2)\alpha$. Therefore there exist no primitive two-sided ideals; every two-sided ideal of $R(2)$ is expressible in one of the two forms: $A^n\cdot BA^n$. Remark that every two-sided $R(2)$-ideal is invariant under the canonical involution of $K(2)$.

The zeta-function of the order $R(p)$ is defined by $\zeta_p(s)=\sum_{n=0}^{\infty} a_n p^{-2ns}$, where a_n is the number of integral right $R(p)$-ideals with norm p^n. Then we have in the case c), $\zeta_2(s)=(1+2\cdot 2^{-2s})(1+2^{-2s}+4^{-2s}+\cdots)=(1+2^{1-2s})(1-2^{-2s})^{-1}$; in the case d) and $m\equiv 2 \pmod 8$, $\zeta_2(s)=(1+2^{-2s}+4\cdot 4^{-2s})(1+2^{-2s}+4^{-2s}+\cdots)=(1+2^{-2s}+4^{1-2s})(1-2^{-2s})^{-1}$; in the case d) and $m\equiv 6 \pmod 8$, $\zeta_2(s)=(1+2^{-2s}+8\cdot 8^{-2s}+16\cdot 16^{-2s}+\cdots)(1+2^{-2s}+4^{-2s}+\cdots)=(1-2^{-2s}-2\cdot 4^{-2s}+8^{1-2s})(1-2^{1-2s})^{-1}(1-2^{-2s})^{-1}$.

§ 5. The number $H'(R)$.

In this section we shall determine the class number $H'(R)$ of the order R along the line of Eichler's paper [1] (R is $\mathfrak{o}+I\mathfrak{o}$ or $\mathfrak{o}+\frac{1}{2}(1+\sqrt{-m}+I)\mathfrak{o}$. (The latter is admitted only in the case $m\equiv 2 \pmod 4$)). Since in the cases c) and d) (see § 4) the level q of the order R has a square factor 4, some modifications are necessary. Let A be any right R-ideal. It has been proved in § 4 that for every rational prime p, the p-adic extension $A(p)$ of A is a principal ideal $\alpha_pR(p)$ with a regular element α_p. Since A is a free $\boldsymbol{Z}$-module contained in

K, A is equal to the intersection of all p-adic extensions of it: $A=\bigcap_p \alpha_p R(p)\cap K$ where α_p is a unit of $R(p)$ except for a finite number of primes p. Conversely, any expression $\bigcap_p \alpha_p R(p)\cap K$, where α_p's are regular elements in $K(p)$, and but for a finite number of primes p, α_p's are units of $R(p)$, gives a right R-ideal (in our sense). Therefore, for the orders $R=\mathfrak{o}+I\mathfrak{o}$ and $R=\mathfrak{o}+\frac{1}{2}(1+\sqrt{-m}+I)\mathfrak{o}$, our definition of right R-ideals is equivalent to that of Eichler. Next, if B is a left R-ideal in our sense, then the p-adic extensions are also principal ideals $R(p)\beta_p$ with regular elements β_p (notice that the conjugate $\bar{B}$ of B is a right R-ideal); and $B=\bigcap_p R(p)\beta_p\cap K$. The left orders of right R-ideals A and the right orders of left R-ideals B are of the form $R'=\bigcap_p \gamma_p R(p)\gamma_p^{-1}\cap K$; we denote by Ω the set of these orders. It is easy to see that for any order $R'\in\Omega$ our definition of right (or left) ideals is equivalent to that of Eichler. Hence the totality of ideals whose right and left orders belong to Ω makes a groupoid with the proper multiplication. Now two orders R' and R'' are said to have the same type if there exists a regular element μ of K such that $R''=\mu R'\mu^{-1}$. Let R_ν $(\nu=1,\cdots,T)$ represent all different types of orders of Ω. The left orders of right R-ideals in the same ideal class have the same type. If two right R-ideals A' and A'' have the same left order R_ν, then $A''=BA'$ with a two-sided R_ν-ideal B. Let $B_{\nu\lambda}$ $(\lambda=1,\cdots,H_\nu)$ be a set of representatives of all classes of two-sided R_ν-ideals. Then we have

$$H'(R)=\sum_{\nu=1}^{T} H_\nu\,.$$

Now the zeta function $\zeta(s)$ of $R(\zeta(s)=\sum_A N(A)^{-2s}$, where the sum extends over all integral right R-ideal A and $N(A)$ denotes the norm of A) is equal to the product of "local" zeta functions $\zeta_p(s)$ of $R(p)$. Since the residue of $\zeta(s)$ at $s=1$ is equal to $q^{-1}\pi^2\sum_{\nu=1}^{T}(H_\nu/e_\nu)$, where $2e_\nu$ is the number of units of R_ν, the so-called mass $M=\sum_{\nu=1}^{T}(H_\nu/e_\nu)$ is expressed explicitly in a "finite" form: $M=\frac{1}{12}\prod_{p\mid q_1}(p-1)\prod_{p\mid q_2}(p+1)$ in the case a), b), or c); the coefficient $\frac{1}{12}$ is replaced by $\frac{1}{6}$ in the case d) (cf. [2]). To obtain a formula for the number $H'(R)$ and $H''(R)$, we need to show the following Lemma which corresponds to Satz 7 of [1]:

LEMMA 6. *Let R_1 and R_2 be two orders of Ω. Let $\mathfrak{o}$ be an order (of rank 2 as a $\boldsymbol{Z}$-module) in a quadratic number field contained in the quaternion algebra K, isomorphic to one of the 4 orders:* $\mathfrak{o}_1=[1,\sqrt{-1}]$, $\mathfrak{o}_2=[1,\frac{1}{2}(1+\sqrt{-3})]$,

$\mathfrak{o}_3=[1, \sqrt{-m}]$, $\mathfrak{o}_4=[1, \frac{1}{2}(1+\sqrt{-m})]$ ($\mathfrak{o}_4$ *appears only in the case a)). Let* $\mathfrak{o}$ *be optimally embedded in* R_i $(i=1, 2)$, *i.e., denoting by* $\boldsymbol{Q}(\mathfrak{o})$ *the quadratic field generated by* $\mathfrak{o}$ *over* $\boldsymbol{Q}$, $\mathfrak{o}=R_i\cap\boldsymbol{Q}(\mathfrak{o})$ $(i=1, 2)$. *Then there exists an ideal* $\mathfrak{a}$ *of* $\mathfrak{o}$ ($\mathfrak{a}$ *having* $\mathfrak{o}$ *as its order) such that* $R_2\mathfrak{a}=\mathfrak{a}R_1$. *And conversely if* $\mathfrak{o}$ *is optimally embedded in the order* R_1 *and if* $\mathfrak{a}$ *is an* $\mathfrak{o}$*-ideal, then* $\mathfrak{o}$ *is optimally embedded in the left order of* $\mathfrak{a}R_1$.

PROOF. The second part can be proved as in the proof of Satz 7 [**1**]. For the first part the assertion as well as assumption are reduced to those for the p-adic extensions. The case in which the level of the orders $R_i(p)$ is square-free, the result is known ([**1**] Satz 7). Hence we have only to consider the case c) $m\equiv 1 \pmod 4$ or d) $m\equiv 2 \pmod 4$ and $R=\mathfrak{o}+I\mathfrak{o}$; $p=2$; and $\mathfrak{o}\cong[1, \sqrt{-1}]$ or $[1, \sqrt{-m}]$ (notice that, since $T_r\left(\frac{1}{2}(1+\sqrt{-3})\right)=1$, $\mathfrak{o}_2$ can not be embedded in $R(2)$). In case c), since every right $R(2)$-ideal is two-sided, we have $R_1(2)=R_2(2)$ and it suffices to take $\mathfrak{a}(2)=\mathfrak{o}(2)$. We consider the case d). Since $R(2)$, $R_1(2)$, $R_2(2)$ are of the same type, by transforming $R_1(2)$ and $R_2(2)$ by a suitable element we may assume $R_1(2)=R(2)$; and that there exists a regular element $\alpha\in K(2)$ such that $R_2(2)=\alpha R(2)\alpha^{-1}$. By the observation in § 4 we may assume that $\alpha=1$ or α is a primitive element of the form: $\alpha=a+bI+\sqrt{-m}\in R(2)$. In the case $\mathfrak{o}\cong\mathfrak{o}_1$ let $J=yI+z\sqrt{-m}+u\sqrt{-m}I$ be the element of $\mathfrak{o}$ which corresponds to $\sqrt{-1}$. Then we have $y^2+mz^2+mu^2=1$ and hence $y\equiv 1$, $z\equiv u\equiv 0 \pmod 2$. Suppose $\alpha\neq 1$. Since $a\equiv b\equiv 1 \pmod 2$, we have $\bar{\alpha}J\alpha\equiv 2y(b+aI)\sqrt{-m}\not\equiv 0 \pmod 4$. This implies $\mathfrak{o}\not\subset R(2)$, a contradiction. Therefore α can not be a primitive element; hence we have $R_2(2)=R(2)$. Next if $\mathfrak{o}\cong\mathfrak{o}_3$ and $J=yI+z\sqrt{-m}+u\sqrt{-m}I$ corresponds to $\sqrt{-m}$, then we have $y^2+mz^2+mu^2=m$ and hence $y\equiv 0 \pmod 2$ and $z-uI$ is a unit of $R(2)$. The congruence $\bar{\alpha}J\alpha\equiv 2(1+I)(z-uI)\sqrt{-m}\not\equiv 0 \pmod 4$ implies that α can not be a primitive element; consequently $R_2(2)=R(2)$. Hence the assertion.

Now the Lemma is proved, so that Eichler's deduction ([**1**] Satz 10) applies to our case. Let R_ν $(1\leq\nu\leq T)$ be an order which represents a type of orders of Ω. We fix a positive rational integer n and observe all elements α_j $(1\leq j\leq c_\nu)$ with norm n in R_ν. With every element α in this set we associate $s=T_r(\alpha)$ and the order $\mathfrak{o}_\nu=R_\nu\cap\boldsymbol{Q}(\alpha)$, where $\boldsymbol{Q}(\alpha)$ is the field generated by α over $\boldsymbol{Q}$. Then $\boldsymbol{Q}(\alpha)$ is a quadratic field and α, $\bar{\alpha}$ determine the same s and $\mathfrak{o}_\nu$, excepting the case $n=a^2$, $a\in\boldsymbol{Z}$, $\alpha=\pm a$. Let $\{\mathfrak{o}_\iota\}$ be the set of mutually non-isomorphic orders $\mathfrak{o}_\iota$ of imaginary quadratic number fields, $\mathfrak{o}_\iota\supset\boldsymbol{Z}[\xi]$, $\xi^2-s\xi+n=0$. We denote by $g_\nu(\mathfrak{o}_\iota)$the number of orders in R_ν which are isomorphic to $\mathfrak{o}_\iota$ and optimally embedded in R_ν (the value $g_\nu=0$ is admitted). We further denote by $\pi_{\nu\nu}(n)$ the number of integral principal right R_ν-ideals with norm n. Then we have

$$\sum_{\nu=1}^{T} H_\nu \pi_{\nu\nu}(n) = \sum_{\nu=1}^{T} (H_\nu c_\nu / 2e_\nu) = (M) + \sum_{s,\iota} \sum_{\nu=1}^{T} (H_\nu g_\nu(\mathfrak{o}_\iota)/e_\nu),$$

where the left hand side is the trace of an "Anzahlmatrix" $P(n)$ (cf. [**1**]), $2e_\nu$ is the number of units of the order R_ν, and (M) is equal to the mass M if n is a square number; $(M)=0$ otherwise. Now, under the assumption that the analogue of Lemma 6 holds for the orders $\mathfrak{o}_\iota$, we can prove in the same way as in [**1**] Satz 10 the following equality (also cf. [**5**]):

$$\sum_{\nu=1}^{T} (H_\nu g_\nu(\mathfrak{o}_\iota)/e_\nu) = \prod_p N_p(\mathfrak{o}_\iota) \cdot \frac{h(\mathfrak{o}_\iota)}{2w(\mathfrak{o}_\iota)} \tag{4}$$

where $h(\mathfrak{o}_\iota)$ is the number of ideal classes of the order $\mathfrak{o}_\iota$, $2w(\mathfrak{o}_\iota)$ is the number of units of the order $\mathfrak{o}_\iota$, and $N_p(\mathfrak{o}_\iota)$ is defined as follows: if $R(p)$ contains an order $\mathfrak{o}'$ isomorphic to $\mathfrak{o}_\iota(p)$ such that $\mathfrak{o}'$ is optimally embedded in $R(p)$, then $N_p(\mathfrak{o}_\iota)$ is equal to the index of the group of those two-sided ideals which are the product of an $\mathfrak{o}'$-ideal and the order $R(p)$, in the group of all two-sided ideals of $R(p)$; if $R(p)$ contains no such order $\mathfrak{o}'$, then $N_p(\mathfrak{o}_\iota)=0$. Now we put $n=1$. Then every element α mentioned above is equal to ± 1 or satisfies the equation $\alpha^2 - s\alpha + 1 = 0$, $s^2 - 4 < 0$. Hence we have only two orders $\mathfrak{o}_1 = [1, \sqrt{-1}]$ and $\mathfrak{o}_2 = [1, \frac{1}{2}(1+\sqrt{-3})]$ to observe as $\mathfrak{o}_\iota$. Then by Lemma 6 the above assumption is satisfied. Since $\pi_{\nu\nu}(1)=1$, the above equality (4) gives $H'(R)$. We have, by [**1**] Satz 10, $N_p = 1$ if $p \nmid q$ $(= q_1 q_2)$; $N_p = 1 - \left\{\frac{\mathfrak{o}_\iota}{p}\right\}$ if $p \| q$, $p | q_1$; $N_p = 1 + \left\{\frac{\mathfrak{o}_\iota}{p}\right\}$ if $p \| q$, $p | q_2$. The symbol $\left\{\frac{\mathfrak{o}}{p}\right\}$ is defined as follows:

$$\left\{\frac{\mathfrak{o}}{p}\right\} = \begin{cases} \left(\frac{k}{p}\right), & \text{if } p \text{ is prime to the conductor of } \mathfrak{o}, \\ 1 & \text{otherwise}; \end{cases}$$

where k is the quadratic field generated by $\mathfrak{o}$ over $\boldsymbol{Q}$ and $\left(\frac{k}{p}\right)$ is the Artin symbol. Since in the cases c) and d) q has a square factor 4, for the value of N_2 the following supplement is necessary:

		$\mathfrak{o}_1$	$\mathfrak{o}_2$	$\mathfrak{o}_3$
Value of N_2	case c)	3	0	3
	case d)	2	0	2

The table is readily verified using the results of § 4. Recalling the fact that an odd prime factor p of $q = q_1 q_2$ divides q_1 if $p \equiv 3 \pmod 4$, and divides q_2 if $p \equiv 1 \pmod 4$, we have the following formulas:

case a) $m \equiv 3 \pmod 4$, $m > 3$,

$$H'(R)=\frac{1}{12}\prod_{p\mid q_1}(p-1)\prod_{p\mid q_2}(p+1)+2^{t-2}+\frac{1}{3}\prod_{p\mid q_1}\left(1-\left(\frac{-3}{p}\right)\right)\prod_{p\mid q_2}\left(1+\left(\frac{-3}{p}\right)\right),$$

case b) $m\equiv 2 \pmod 4$, $m>2$, $R=\mathfrak{o}+\frac{1}{2}(1+\sqrt{-m}+I)\mathfrak{o}$,

$$H'(R)=\frac{1}{12}\prod_{p\mid q_1}(p-1)\prod_{p\mid q_2}(p+1)+2^{t-3}+\frac{1}{3}\prod_{p\mid q_1}\left(1-\left(\frac{-3}{p}\right)\right)\prod_{p\mid q_2}\left(1+\left(\frac{-3}{p}\right)\right),$$

case c) $m\equiv 1 \pmod 4$, $m>1$, $H'(R)=\frac{1}{12}\prod_{p\mid q_1}(p-1)\prod_{p\mid q_2}(p+1)+3\cdot 2^{t-3}$,

case d) $m\equiv 2 \pmod 4$, $m>2$, $R=\mathfrak{o}+I\mathfrak{o}$,

$$H'(R)=\frac{1}{6}\prod_{p\mid q_1}(p-1)\prod_{p\mid q_2}(p+1)+2^{t-2},$$

where t is the number of distinct prime factors of the discriminant of the principal order $\mathfrak{o}$ of $\boldsymbol{Q}\sqrt{-m}$).

§ 6. The number of singular classes.

Every class C of right R-ideal ($R=\mathfrak{o}+I\mathfrak{o}$ or $R=\mathfrak{o}+\frac{1}{2}(1+\sqrt{-m}+I)\mathfrak{o}$, $m\equiv 2 \pmod 4$) contains a right R-ideal of the form $A=k\mathfrak{o}+(\alpha+I)\mathfrak{o}$ where $k\in\boldsymbol{Z}$. $\alpha\in\mathfrak{o}$, $k>0$, $k\mid\alpha\bar{\alpha}+1$ (§ 3). It is easy to see that the class C is singular if and only if two right R-ideals A and $A'=k\mathfrak{o}+(\alpha-I)\mathfrak{o}$ are equivalent. Since $A'=\sqrt{-m}^{-1}A\sqrt{-m}$, the condition is equivalent to the equivalence of two right ideals A and $A\sqrt{-m}$.

LEMMA 7. *Let $m>3$. A right R-ideal A belongs to a singular class if and only if the left order of A contains an element λ satisfying the equation $\lambda^2+m=0$.*

PROOF. Suppose A belongs to a singular class. Then there exists an element $\lambda\in K$ such that $\lambda\cdot A=A\sqrt{-m}$. We have $\lambda\bar{\lambda}=m$; and the element λ belongs to the left order R', say, of A. Now we have $\bar{\lambda}A\sqrt{-m}=\bar{\lambda}\lambda A=Am$ and hence $\bar{\lambda}A=A\sqrt{-m}=\lambda A$. Therefore there exists a unit ε of R' such that $\bar{\lambda}=\lambda\varepsilon$. We have $\boldsymbol{Q}(\varepsilon)\subset\boldsymbol{Q}(\lambda)$. If ε does not belong to $\boldsymbol{Q}$, then we have $\boldsymbol{Q}(\varepsilon)=\boldsymbol{Q}(\lambda)$. Since K is a definite quaternion algebra, $\boldsymbol{Q}(\varepsilon)$ is an imaginary quadratic field and ε satisfies the following equation: $\varepsilon^2-a\varepsilon+1=0$, $a=0$ or ±1. We can put $\bar{\lambda}=x+y\varepsilon$, with $x, y\in\boldsymbol{Z}$, and the above relation implies that $x=y$. Then we have $m=\lambda\bar{\lambda}=x^2N(1+\varepsilon)$. Since $N(1+\varepsilon)=1$, 2, or 3, and since we are assuming m is square-free and $m>3$, this is impossible. Hence $\varepsilon\in\boldsymbol{Q}$, i.e. $\varepsilon=\pm1$, If $\varepsilon=1$ then $\lambda\in\boldsymbol{Z}$ and m is a square number. This is impossible. Therefore we have $\varepsilon=-1$ and λ satisfies the equation $\lambda^2+m=0$. Conversely suppose the left order R' of A contains an element λ which satisfies the equation $\lambda^2+m=0$. Then $\lambda R'(p)=R'(p)\lambda$ for all p (§ 4), so that $\lambda R'=R'\lambda$.

$A^{-1}\lambda A$ is an integral two-sided R-ideal with norm m. In the case a), b), or c), there exists no such an ideal of R except $R\sqrt{-m}$, and hence we have $\lambda A = A\sqrt{-m}$. In the case d), there exist just two such ideals $R\sqrt{-m}$ and B, say, where the 2-adic extension $B(2)$ of B is $(1+I)R(2)$. By Lemma 5 there exists an element $C \in K(2)$ such that $A(2) = CR(2)$. The element $C^{-1}\lambda C$ belongs to the 2-adic extension of $A^{-1}\lambda A$. Putting $C^{-1}\lambda C = x+yI+z\sqrt{-m}+u\sqrt{-m}I$, $x, y, z, u \in \boldsymbol{Z}(2)$, we have $T_r(C^{-1}\lambda C) = 2x = 0$, $n(C^{-1}\lambda C) = y^2+mz^2+mu^2 = m$. If $C^{-1}\lambda C \in (1+I)R(2)$, then $y \equiv 0$, $z \equiv u \pmod 2$ and consequently $y^2+mz^2+mu^2 \equiv 0 \pmod 4$. Since $m \not\equiv 0 \pmod 4$, this is impossible. Hence the 2-adic extension of $A^{-1}\lambda A$ is $R(2)\sqrt{-m}$; and we have $A^{-1}\lambda A = R\sqrt{-m}$. This completes the proof.

LEMMA 8. *Let R' be the left order of some righ R-ideal (i.e. $R' \in \Omega$). If R' contains an element λ satisfying the equation $\lambda^2+m=0$, then for any unit ε of R', $\lambda\varepsilon$ satisfies the equation $\lambda^2+m=0$; and every root $\mu \in R'$ of this equation is obtained in this way.*

PROOF. This is easily seen from the proof of Lemma 7.

Now let $R_1, \cdots, R_T$ be a set of orders representing the all different types of orders of Ω. Suppose an order R_ν contains an element λ which satisfies the equation $\lambda^2+m=0$. Then by Lemma 8, the number of roots μ $(\in R_\nu)$ of this equation is equal to the number $2e_\nu$ of units of R_ν. With every root $\mu \in R_\nu$ of this equation we associate an order $\mathfrak{o}_\mu = R_\nu \cap Q(\mu)$. Then every order $\mathfrak{o}_\mu$ corresponds to just two roots $\pm\mu$; and $\mathfrak{o}_\mu$ is isomorphic to $\mathfrak{o}_3 = [1, \sqrt{-m}]$ or $\mathfrak{o}_4 = [1, \frac{1}{2}(1+\sqrt{-m})]$ (the latter case may occur only in the case a)). Hence we have the equality $e_\nu = g_\nu(\mathfrak{o}_3)+g_\nu(\mathfrak{o}_4)$ in the case a), and $e_\nu = g_\nu(\mathfrak{o}_3)$ in the case b), c), or d). If an order R_ν does not contain such an element λ, then of course we have $g_\nu(\mathfrak{o}_3) = g_\nu(\mathfrak{o}_4) = 0$. Now we have an expression of $H''(R):H''(R) = \sum_{\iota=3,4}\sum_{1\leqq\nu\leqq T}(H_\nu g_\nu(\mathfrak{o}_\iota)/e_\nu)$. On account of Lemma 6 we can apply the formula (4) in § 5 to this expression. Using the values of N_p in § 5, and noticing that $h(\mathfrak{o}_3) = (2-\chi(2))h(\mathfrak{o}_4)$, where χ is the Artin symbol for $\boldsymbol{Q}(\sqrt{-m})/\boldsymbol{Q}$, we have the following results: the number $H''(R)$ of singular classes of the order R is $\frac{1}{2}(3-\chi(2))h(\mathfrak{o}_4)$ in the case a); $\frac{1}{2}h(\mathfrak{o}_3)$ in the case b); $\frac{3}{2}h(\mathfrak{o}_3)$ in the case c); $h(\mathfrak{o}_3)$ in the case d) $(m>3)$.

§ 7. Class number formulas.

We summarize our calculations in the following formulas for H which is introduced at the beginning of this paper. We have:

I. If $m \equiv 3 \pmod 4$ and $m>3$, then

$$H=\frac{1}{24}\prod_{p\mid q_1}(p-1)\prod_{p\mid q_2}(p+1)$$
$$+\frac{1}{6}\prod_{p\mid q_1}\left(1-\left(\frac{p}{3}\right)\right)\prod_{p\mid q_2}\left(1+\left(\frac{p}{3}\right)\right)+\frac{1}{4}(1-(-1))^{\frac{1}{8}(m^2-1)}-2^{t-3}.$$

II. If $m\equiv 1 \pmod 4$ and $m>1$, then

$$H=\frac{1}{8}\prod_{p\mid q_1}{}'(p-1)\prod_{p\mid q_2}{}'(p+1)+\frac{1}{4}h-2^{t-4}.$$

III. If $m\equiv 2 \pmod 8$ and $m>2$, then

$$H=\frac{7}{24}\prod_{p\mid p_1}{}'(p-1)\prod_{p\mid q_2}{}'(p+1)$$
$$+\frac{1}{3}\prod_{p\mid q_1}{}'\left(1-\left(\frac{p}{3}\right)\right)\prod_{p\mid q_2}{}'\left(1+\left(\frac{p}{3}\right)\right)+\frac{1}{4}h-2^{t-4}.$$

IV. If $m\equiv 6 \pmod 8$, then

$$H=\frac{3}{8}\prod_{p\mid q_1}(p-1)\prod_{p\mid q_2}{}'(p+1)+\frac{1}{4}h-2^{t-4}.$$

where $\prod'$ indicates that the product extends over only odd prime factors of q_i $(i=1$ or $2)$, i.e. the first product extends over all prime factors $p\equiv -1$ (mod 4) of m, and the second over all prime factors $p\equiv 1$ (mod 4) of m; h and t are the class number and the number of distinct prime factors of the principal order of $Q(\sqrt{-m})$; and $\left(\frac{p}{3}\right)$ is the Legendre symbol. In the excluded cases $m=0, 1, 2, 3$, we know $H=0, 0, 1, 0$, respectively [3].

Ochanomizu University

Bibliography

[1] M. Eichler, Zur Zahlentheorie der Quaternionen-Algebren, J. Reine Angew. Math., **195** (1955), 127–151.

[2] M. Eichler, Über die Idealklassenzahl total definiter Quaternionenalgebren, Math. Z., **43** (1938), 102–109.

[3] T. Hayashida and M. Nishi, Existence of curves of genus two on a product of two elliptic curves, J. Math. Soc. Japan, **17** (1965), 1–16.

[4] T. Hayashida, A class number associated with a product of two elliptic curves, Nat. Sci. Rep. Ochanomizu Univ., **16** (1965), 9–19.

[5] V. Kořínek, Kvadratická tělesa v kvaternionových okruzích, Věst. Král. Česke Spol. Nauk, Tř. II, 1930, 1–46.

[6] M. Nishi, Some results on abelian varieties, Nat. Sci. Rep. Ochanomizu Univ., **9** (1958), 1–12.

[7] A. Weil, Zum Beweis des Torellischen Satzes, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl., (1957), 33–53.