Natural Science Report, Ochanomizu University, Vol. 16, No. 1, 1965
お茶の水女子大学 自然科学報告 第16巻 第1号

A Class Number Associated with a Product of Two Elliptic Curves

Tsuyoshi Hayashida (林 田 侃)

Department of Mathematics, Faculty of Science
Ochanomizu University, Tokyo

(*Received April 10, 1965*)

In this paper we shall consider the product $E\times E'$ of two mutually isogenous elliptic curves E, E' whose rings of endomorphisms are the ring Z of rational integers. We ask whether $E\times E'$ can be a Jacobian variety of some curve; and further in how many essentially different ways. In other words we try to obtain a formula for the number H of isomorphism classes of canonically polarized Jacobian varieties $(E\times E', Y)$, Y being a theta divisor. The number H proves to be closely connected with the number of ideal classes and the number of ambiguous ideal classes of a certain imaginary quadratic field $Q(\sqrt{-m})$ [§ 8]. The method of this paper is basically the same as that of a study [2], in which the rings of endomorphisms of E, E' are the principal order of an imaginary quadratic field. I wish to express here my hearty thanks to my friend M. Nishi for his suggestions and encouragement.

§1. Basic homomorphism. Let E and E' be two mutually isogenous elliptic curves whose rings of endomorphisms are isomorphic to the ring Z of rational integers. We denote by $H(E, E')$ the set of all homomorphisms of E on E'. Then it is easy to see that $H(E, E')$ is a module isomorphic to Z; namely there is a basic homomorphism $\tau\in H(E, E')$ such that every element λ of $H(E, E')$ is an integral multiple of τ: $\lambda=n\tau$, $n\in Z$. Obviously τ is a homomorphism of the minimal degree: $\nu(\tau)\leqq\nu(\lambda)$. We know that there is a homomorphism τ' of E' on E such that $\tau'\circ\tau=m\delta_E$, $\tau\circ\tau'=m\delta_{E'}$, where $m=\nu(\tau)=\nu(\tau')$ and δ_E (resp. $\delta_{E'}$) is the identity map of E (resp. E'); the number m is determined uniquely by a pair $\{E, E'\}$. We shall show

LEMMA 1. *Notations being as above, either τ or τ' is a separable homomorphism whose kernel is a cyclic group of order m.*

PROOF. First we shall show that the kernel $\mathfrak{g}$ of τ is a cyclic group. Since $dim\, E=1$, by the fundamental theorem of finite abelian groups, $\mathfrak{g}$ is a direct product of two cyclic groups of orders n_1 and n_2,

where we may assume $n_1 \mid n_2$. If $n_1 > 1$, then $\mathfrak{g}$ contains the kernel of the endomorphism $n_1\delta_E$. This means that there exists a homomorphism μ of E on E' such that $\mu \circ n_1\delta_E = \tau$; this contradicts to the fact that τ is a basic element of $H(E, E')$. Hence $n_1 = 1$ and $\mathfrak{g}$ is a cyclic group. By the same reason the kernel of τ' is a cyclic group. Next suppose the characteristic p is positive and τ inseparable. Let k be a common field of definition of E, E', τ, and x a generic point of E over k. We may assume that k is algebraically closed. Then the inseparability of τ means that $k(x^p) \supset k(\tau x)$. Now it is known that the endomorphism $p\delta_E$ of E is inseparable and its kernel is isomorphic to a cyclic group of order p[1]. Therefore, if $\mathfrak{g}$ contains a cyclic group of order p, then $k(px)$ contains $k(\tau x)$, so that the correspondence $E \ni px \to \tau x \in E'$ gives a homomorphism μ of E on E' such that $\nu(\mu) < \nu(\tau)$. Since τ is a basic element of $H(E, E')$, this is a contradiction. Hence the order of $\mathfrak{g}$ is relatively prime to p. We know that there is a positive integer n such that τ is a composed map of two homomorphisms defined by the correspondences $E \ni x \to x^{p^n} \in E^{p^n}$ and $E^{p^n} \ni x^{p^n} \to \tau x \in E'$, the degree of the latter homomorphism being prime to p. Then we can see that τ' is a composed map of two homomorphisms: a homomorphism of E' on E^{p^n}, of degree $[k(x^{p^n}) : k(\tau x)]$, and that of E^{p^n} on E, of degree p^n; both are separable. Hence τ' is separable and the proof is completed.

§ 2. Elliptic curves on $E \times E'$. Now we consider the product $E \times E'$. Transposing E and E' if necessary, we may assume without loss of generality, that τ is separable. For any two integers a, b, $\{a, b\} \neq \{0, 0\}$, the correspondence

$$h_{a,b\tau} : E \ni x \to (ax, b\tau x) \in E \times E'$$

defines a homomorphism of E into $E \times E'$. The image of E by $h_{a,b\tau}$ is an abelian subvariety of dimension 1 on $E \times E'$, namely an elliptic curve lying on $E \times E'$; we denote it by $E_{a,b\tau}$. It is clear that translations of $E_{a,b\tau}$ also are elliptic curves on $E \times E'$. Conversely we can see that every elliptic curve on $E \times E'$ is a translation of some $E_{a,b\tau}$[2]. In order to calculate intersection numbers of divisors on $E \times E'$ we need some lemmas.

LEMMA 2. $\nu(h_{a,b\tau}) = (a^2, ab, mb^2)$.

PROOF. Putting $(a, b) = d$, $a = a'd$, $b = b'd$, we have $h_{a,b\tau} = h_{a',b'\tau} \circ d\delta_E$, and $\nu(h_{a,b\tau}) = d^2\nu(h_{a',b'\tau})$. Hence, dividing both sides of the above equality by d^2 and replacing a', b' by a, b respectively, we may assume that $(a, b) = 1$. Let k be a field over which E, E', τ are defined, and x a

1) If $p\delta_E$ were purely inseparable, then $H(E, E) \otimes Q$ would be a quaternion algebra over Q. See Deuring [1].

2) The proof of this is similar to that of Lemma 1 in [2].

generic point of E over k. Then $\nu(h_{a,b\tau})=[k(x):k(ax, b\tau x)]$. Since $(a, b)=1$, we have $k(ax, b\tau x)=k(ax, a\tau x, b\tau x)=k(ax, \tau x)$; and $(a^2, ab, mb^2)=(a, b)(a, mb)=(a, m)$. Hence we may further assume that $b=1$. Now $h_{a,\tau}$ is separable. Hence $\nu(h_{a,\tau})$ is the order of the kernel $\mathfrak{g}_1$ of $h_{a,\tau}$. We know that $\mathfrak{g}_1$ is the intersection of the kernels of $a\delta_E$ and τ; consequently $\mathfrak{g}_1$ is composed of all elements of the kernel of τ whose orders divide a. Therefore we have $\nu(h_{a,\tau})=(a, m)$. This completes our proof.

LEMMA 3. *Let x and y be two independent generic points of E over a field k. Assume $ad-bc\neq 0$; $a, b, c, d\in Z$. Then*

$$[k(x):k(ax+by, cx+dy)]=(ad-bc)^2$$

This lemma is a special case of Lemma 2 [2], so we omit the proof here.

Now every endomorphism of $E\times E'$ is given by the following correspondence

$$E\times E'\ni(x, \tau y)\rightarrow(px+mry, \tau qx+\tau sy)\in E\times E'$$

where $x, y\in E$; $p, q, r, s\in Z$. We may represent this endomorphism by a matrix $\begin{pmatrix} p & mr \\ q & s \end{pmatrix}$.

COROLLARY OF LEMMA 3. $\nu\begin{pmatrix} p & mr \\ q & s \end{pmatrix}=(ps-mqr)^2$.

PROOF. If $ps-mqr=0$, then the endomorphism is into and both sides of the equality are zero. Assume $ps-mqr\neq 0$. Let x and y be two independent generic points of E over a field k over which E' and τ are defined. Then by Lemma 3, $px+mry$ and $qx+sy$ are independent generic points of E over k and the endomorphism is onto. The left hand side is equal to $[k(x, \tau y); k(px+mry, \tau qx+\tau sy)]$. Our assertion follows immediately from Lemma 3.

On account of Corollary of Lemma 3 the endomorphism $\begin{pmatrix} p & mr \\ q & s \end{pmatrix}$ is an automorphism if and only if $ps-mgr=\pm 1$.

In what follows we denote by (X, Y) the intersection number of divisors X and Y on $E\times E'$.

LEMMA 4. $(E_{a,b\tau}, E_{c,d\tau})=\dfrac{(ad-bc)^2m}{N(a, b\tau)N(c, d\tau)}$ *where we put* $(a^2, ab, mb^2)=N(a, b\tau)$ *etc. (for brevity's sake).*

PROOF. If $ad-bc=0$, then we have $E_{a,b\tau}=E_{c,d\tau}$ and the above equality clearly holds. Assume $ad-bc\neq 0$. Let k be a field of definition for E, E' and τ; and x and y be two independent generic points of E over k. Then by Weil [7] Cor. 2 of Th. 4

$$[E_{a,b\tau}, E_{c,d\tau}]=[k(ax, b\tau x, cy, d\tau y) : k(ax+cy, b\tau x+d\tau y)]$$

$$=\frac{[k(x, y) : k(u, v)][k(u, v) : k(u, \tau v)]}{[k(x) : k(ax, b\tau x)][k(y) : k(cy, d\tau y)]}$$

where we put $u=ax+cy$, $v=bx+dy$. Our assertion now follows from Lemmas 2 and 3.

COROLLARY 1. $E_{a,b\tau}=E_{c,d\tau}$ if and only if $ad-bc=0$.

PROOF. The "if" part is obvious. The "only if" part follows from Lemma 4.

COROLLARY 2. $(E_{a,b\tau}, E_{c,d\tau})=1$ with $(a, b)=(c, d)=1$ if and only if $ad-bc=\pm 1$ and $m=(a, m)(c, m)$.

PROOF. If $ad-bc=\pm 1$, then clearly $(a, b)=(c, d)=1$. So we are assuming $(a, b)=(c, d)=1$ in both directions. Then by Lemma 4, $(E_{a,b\tau}, E_{c,d\tau})=1$ if and only if $(ad-bc)^2m=(a, m)(c, m)$. The last equality implies that $(ad-bc)^2$ divides both (a, m) and (c, m); consequently $(ad-bc)^2 \mid (a, c, m) \mid ad-bc$. This means that $ad-bc=\pm 1$. The rest is obvious.

Now suppose $(E_{a,b\tau}, E_{c,d\tau})=1$. Then by Weil [7] Cor. 2 of Th. 4, $E_{a,b\tau}\times E_{c,d\tau}$ is isomorphic to $E\times E'$; moreover the isomorphism is given by the correspondence

$$E_{a,b\tau}\times E_{c,d\tau}\ni(P, Q)\longrightarrow P+Q\in E\times E'$$

Assuming that $(a, b)=(c, d)=1$ (there is no loss of generality in so doing), there is a separable homomorphism of E on $E_{a,b\tau}$ (resp. $E_{c,d\tau}$) whose kernel is a cyclic group of order (a, m) (resp. (c, m)). Since by Corollary 2, (a, m) and (c, m) are relatively prime and $(a, m)(c, m)=m$, there is a separable homomorphism either of $E_{a,b\tau}$ on $E_{c,d\tau}$ or of $E_{c,d\tau}$ on $E_{a,b\tau}$ whose kernel is a cyclic group of order m. This shows that the number m is an invariant of the isomorphism class of $E\times E'$.

Another application of Corollary 2. It is easy to see that for a given elliptic curve $E_{a,b\tau}$, $(a, b)=1$, there is an elliptic curve $E_{c,d\tau}$ such that $(E_{a,b\tau}, E_{c,d\tau})=1$ if and only if (a, m) and $m/(a, m)$ are relatively prime. We can conclude from this that a necessary and sufficient condition that every elliptic curve $E_{a,b\tau}$ shall have a "partner" $E_{c,d\tau}$ on $E\times E'$ such that $(E_{a,b\tau}, E_{c,d\tau})=1$ is that m has no squared factor.

§ 3. Intersection numbers. Now any divisor X on $E\times E'$ is algebraically equivalent to a linear combination of elliptic curves $E_{1,0}(=E\times 0)$, $E_{0,\tau}(=0\times E')$ and $E_{1,\tau}$ which is the graph of a basic homomorphism τ of E on E' (cf. Weil [7], Th. 22):

$$X\equiv qE_{1,0}+rE_{0,\tau}+sE_{1,\tau} \quad (q, r, s\in Z) \tag{1}$$

Since the intersection number $(X, E_{c,d\tau})$ is linear with respect to X,

we know by Lemma 4 that there are constants k_1, g_1, l_1 depending only on X such that

$$(X, E_{c,d\tau})=\frac{1}{N(c, d\tau)}(k_1c^2-2g_1cd+l_1d^2) \tag{2}$$

for every $E_{c,d\tau}$. We can easily see that constants k_1, g_1, l_1 are uniquely determined by X. We attach a matrix

$$M(X)=\begin{pmatrix} k_1 & -g_1 \\ -g_1 & l_1 \end{pmatrix} \tag{3}$$

to any divisor X. Then $M(X)=0$ if and only if $X\equiv 0$. And we have

$$M(E_{a,b\tau})=\frac{m}{N(a, b\tau)}\begin{pmatrix} b^2 & -ab \\ -ab & a^2 \end{pmatrix}. \tag{4}$$

For divisor (1) we have $M(X)=\begin{pmatrix} r+ms & -ms \\ -ms & mq+ms \end{pmatrix}$. This implies in particular that k_1, g_1, l_1 in (3) are three integers satisfying the congruences $g_1\equiv l_1\equiv 0 \pmod m$; and that conversely for any such three integers k_1, g_1, l_1 there exists a divisor X on $E\times E'$ for which (3) holds. We can write

$$M(X)=\begin{pmatrix} k & -mg \\ -mg & ml \end{pmatrix} \quad (k, g, l\in Z) \tag{3'}$$

Let X, Y be any two divisors. Since (X, Y) is linear with respect to Y, by (2), (4) we have $(X, Y)=kl'+lk'-2mgg'$, where $M(Y)=\begin{pmatrix} k' & -mg' \\ -mg' & ml' \end{pmatrix}$. Putting $X=Y$, we have

$$\frac{1}{2}(X, X)=kl-mg^2=\frac{1}{m}\det M(X). \tag{5}$$

§ 4. Divisors with self intersection number 2. Let X be a divisor on $E\times E'$ and put $M(X)=\begin{pmatrix} k & -mg \\ -mg & ml \end{pmatrix}$. Suppose X is algebraically equivalent to a divisor Y, $Y>0$, $(Y, Y)=2$. Then $M(X)=M(Y)$, and by (5) we have $kl-mg^2=1$ (this implies $k\neq 0$), and by (2) $k=(Y, E_{1,0})>0$. We consider the converse. Let k, g, l be integers such that $k>0$ and $kl-mg^2=1$; and X a divisor on $E\times E'$ such that $M(X)$ is given by (3'). Then we have $(X, X)=2$ and $(X, E_{1,0})>0$. Now the following lemma holds.

LEMMA 5. *Let X be a divior on $E\times E'$ such that $(X, X)=2$. Then either $l(X)\geqq 1$, $l(-X)=0$ or $l(-X)=1$, $l(X)=0$. ($l(X)$ means the dimension of the complete linear system $|X|$.)*

PROOF. The proof is similar to that of Lemma 4 in [2]. It runs as follows: Since the arithmetic genus of an abelian variety is zero (cf. Nishi [4]), it follows from the theorem of Riemann-Roch in Serre

[5] that $l(X)+l(-X)\geqq-\chi_{E\times E'}(X)$, where $\chi_{E\times E'}(X)$ means the virtual arithmetic genus of X. By Nishi [4] Theorem 6, $\chi_{E\times E'}(X)=-\frac{1}{2}(X, X)$ for any divisor X on $E\times E'$. Combining these two facts and our assumption, we obtain the desired result.

Returning to our case, by means of this lemma we know that either $l(X)\geqq 1$ or $l(-X)\geqq 1$. Since $(X, E_{1,0})>0$, the latter case can not occur. Therefore there exists a positive divisor Y linearly equivalent to X.

Next suppose Y and Y' are two positive divisors on $E\times E'$ such that $Y\equiv Y'$ and $(Y, Y)=2$. Now Nishi [4] Theorem 6 and its Corollaries implies the following

LEMMA 6. *Let Y be a positive divisor on $E\times E'$ such that $(Y, Y)>0$; then Y is non-degenerate and $l(Y)=1/2(Y, Y)$.*

Then by Lemma 6 and by our assumptions, there exists $t\in E\times E'$ such that $Y\sim Y'_t$; and $l(Y)=1$. Whence $Y=Y'_t$, namely Y is a translation of Y'.

We have seen that to any matrix $\begin{pmatrix} k & -mg \\ -mg & ml \end{pmatrix}$, $k, g, l\in Z$, $k>0$, $kl-mg^2=1$, there corresponds a positive divisor Y, with the self intersection number 2, on $E\times E'$, such that $M(Y)=\begin{pmatrix} k & -mg \\ -mg & ml \end{pmatrix}$, and conversely; and by each such matrix, Y is uniquely determined up to translations.

§ 5. The problem. Now we ask in how many essentially different ways $E\times E'$ can be a Jacobian variety. In other words, we try to obtain the number of isomorphism classes of canonically polarized Jacobian varieties $(E\times E', Y)$. The base of our calculation is the following

LEMMA 7. (cf. Weil [8] Satz 2) *Let Y be a positive non-degenerate divisor on $E\times E'$ such that $(Y, Y)=2$. Then, either Y is irreducible and $E\times E'$ 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 introduce an equivalence relation $A^{-1}(Y)\equiv Y'$ in the set of all positive divisors Y with $(Y, Y)=2$, where A is an automorphism of $E\times E'$. We shall see below that the number of these equivalence classes is finite; we denote it by h_1. If Y is irreducible, then by virtue of Lemma 7, 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 by Torelli's theorem two such curves are birationally equivalent to each other if and only if they are equivalent in the above mentioned sense; we denote by H the number of equivalence classes which con-

tain positive irreducible divisors Y, $(Y, Y)=2$. Finally we denote by h_2 the number of equivalence classes which cantain sums of two elliptic curves E_1+E_2, $(E_1, E_2)=1$. Then, by virture of Lemma 7 we have $H=h_1-h_2$.

Suppose an automorphism A of $E\times E'$ is given by the correspondense described before Corollary of Lemma 3. Then it is easy to see that the condition $A^{-1}(Y)\equiv Y'$ is written in the following form:

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

This determines an equivalence relation in the set of matrices $M(Y)$, where $Y>0$, $(Y, Y)=2$. We now associate a quadratic form $kx^2-2mgxy+mly^2$ with $M(Y)=\begin{pmatrix} k & -mg \\ -mg & ml \end{pmatrix}$. This is a positive primitive (i. e. $(k, -mg, ml)=1$) quadratic form of determinant m. Since $ps-mqr=\pm 1$, with equivalent matrices there are associated quadratic forms in the same class. Now first we show that any class of positive primitive quadratic forms of determinant m contains at least one form associated with some $M(Y)$, $Y>0$, $(Y, Y)=2$. To prove this, suppose a form $F=Ax^2+2Bxy+Cy^2$ with $AC-B^2=m$, $(A, B, C)=1$, $A>0$, is given. Then there are two integers, x_0, y_0, prime to each other, such that $Ax_0^2+2Bx_0y_0+Cy_0^2$ is prime to m[3]. Hence, applying a unimodular transformation to F if necessary, we may assume that A is prime to m. Then a substitution $x=x'+ry'$, $y=y'$ with $Ar+B\equiv 0 \pmod m$ takes F into a form $A'x'^2+2B'x'y'+C'y'^2$ such that $B'\equiv C'\equiv 0 \pmod m$. Next we show that if quadratic forms F, F', associated with matrices $M(Y)$, $M(Y')$ respectively, are in the same class, then these two matrices are equivalent to each other in the above mentioned sense. To prove this it is sufficient to see that the equality

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} k & -mg \\ -mg & ml \end{pmatrix} \begin{pmatrix} p & r \\ q & s \end{pmatrix} = \begin{pmatrix} k' & -mg' \\ -mg' & ml' \end{pmatrix}$$

where $ps-qr=\pm 1$, $kl-mg^2=1$, implies that $r\equiv 0 \pmod m$. By considering both sides modulo m, this readily follows.

We have seen that there is a one to one correspondence between the above mentioned equivalence classes of divisors Y, $Y>0$, $(Y, Y)=2$, (i. e. isomorphism classes of polarized abelian varieties $(E\times E', Y)$) and classes of positive primitive quadratic forms of determinant m. This in particular implies that h_1 is finite.

§ 6. Calculation of h_2. Let $E_{a,b\tau}$ and $E_{c,d\tau}$ be two elliptic curves on $E\times E'$. By Corollary 1 of Lemma 4, we may assume without loss of generality, that $(a, b)=(c, d)=1$. Then by Corollary 2 of Lemma 4,

3) See for example Mathews' book: Theory of numbers, Art. 127.

$(E_{a,b\tau}, E_{c,d\tau})=1$ if and only if $ad-bc=\pm 1$ and $(a, m)(c, m)=m$. Putting $(a, m)=m_1$, $(c, m)=m_2$ we have

$$M(E_{a,b\tau}+E_{c,d\tau})=m_2\begin{pmatrix} b^2 & -ab \\ -ab & a^2 \end{pmatrix}+m_1\begin{pmatrix} d^2 & -cd \\ -cd & c^2 \end{pmatrix}$$

$$=\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} m_1 & 0 \\ 0 & m_2 \end{pmatrix}\begin{pmatrix} d & -c \\ -b & a \end{pmatrix}.$$

Hence we know that the quadratic form associated with $M(E_{a,b\tau}+E_{c,d\tau})$ is equivalent to a quadratic form $m_1x^2+m_2y^2$, where $m_1m_2=m$, $(m_1, m_2)=1$. Conversely suppose any two positive integers m_1, m_2 for which $m_1m_2=m$, $(m_1, m_2)=1$, are given. Then there exist integers b, d such that $m_1d-m_2b=1$; and the quadratic form associated with $M(E_{m_1,b\tau}+E_{m_2,d\tau})$ is equivalent to $m_1x^2+m_2y^2$. Moreover, if two positive forms $m_1x^2+m_2y^2$, and $n_1x^2+n_2y^2$ with $m_1m_2=n_1n_2=m$, $(m_1, m_2)=(n_1, n_2)=1$, are equivalent, then either $m_1=n_1$, $m_2=n_2$ or $m_1=n_2$, $m_2=n_1$. (Notice that if $m_1\leqq m_2$, then m_1 is the least positive integer represented by $m_1x^2+m_2y^2$.) From these we know that h_2 is equal to the number of factorizations of m such that $m=m_1m_2$, $m_1>0$, $(m_1, m_2)=1$. Thus we have

$$h_2=\begin{cases} 1 & (\text{if } m=1) \\ 2^{t-1} & (\text{if } m>1) \end{cases}$$

where t is the number of prime factors of m.

§ 7. Calculation of h_1. Class number formulas for quadratic forms are classical. For completeness we shall briefly note a way of reduction and state the results.

Two quadratic forms F, F' are said to be properly equivalent to each other if there exists a tranformation with determinant 1 which takes F into F'. Then the number of proper equivalence classes contained in a class of quadratic forms is one or two. In the former case the class is said to be self conjugate (or ambiguous). We denote by H_1 the number of proper equivalence classes of positive primitive quadratic forms of determinant m; and by H_2 that of self conjugate classes. Then we have $h_1=\frac{1}{2}(H_1+H_2)$.

CALCULATION of H_1. Put $m=f^2m_0$, where m_0 is square free. We distinguish two cases according as $m_0\equiv 1$ or 2; or $3 \pmod 4$.

CASE I. $m_0\equiv 1$ or $2 \pmod 4$. In this case all forms are properly primitive: $(A, 2B, C)=1$. Let $R=[1, \sqrt{-m}]$ be the ring of all integers of the form $x+y\sqrt{-m}$ $(x, y\in Z)$; and by $\mathfrak{o}$ the principal order of $Q(\sqrt{-m_0})$. Then the conductor $\mathfrak{f}$ of R is $f\mathfrak{o}$. There is a one to one correspondence between proper equivalence classes of positive primitive quadratic forms $F(x, y)$ of determinant m and classes of regular

ideals $\mathfrak{a}=[\alpha_1, \alpha_2]$ of R, such that $N(\alpha_1 x+\alpha_2 y)=N\mathfrak{a}F(x, y)$, $Im(\alpha_2/\alpha_1)>0$. Again, there is a one to one correspondence between regular ideals $\mathfrak{a}$ in R and ideals $\mathfrak{a}_0$ of $\mathfrak{o}$, relatively prime to the conductor $f\mathfrak{o}$, such that $\mathfrak{a}\mathfrak{o}=\mathfrak{a}_0$, $\mathfrak{a}_0\cap R=\mathfrak{a}$. The correspondence $\mathfrak{a}\to\mathfrak{a}_0$ determines a homomorphism of the class group of (regular) ideals of R on that of $\mathfrak{o}$. We denote by K the order of the kernel of this homomorphism. Let α be an element of $\mathfrak{o}$ which is prime to $f\mathfrak{o}$. Then $\alpha\mathfrak{o}\cap R$ is a principal ideal of R if and only if there exists a rational integer r and a unit ε of $\mathfrak{o}$ such that $\alpha\equiv r\varepsilon \pmod{f\mathfrak{o}}$. Whence we can conclude that

$$H_1=Kh,\quad K=\begin{cases}\dfrac{2f}{w}\displaystyle\prod_{p\mid f}\left(1-\frac{\chi(p)}{p}\right) & (\text{if } m>1)\\ 1 & (\text{if } m=1)\end{cases}$$

where w is the number of units of $\mathfrak{o}$; $\chi(p)$ is the Kronecker symbol for $Q(\sqrt{-m_0})$; and h is the number of ideal classes of $\mathfrak{o}$; and the product extends over all prime factors of f.

CASE II $m_0\equiv 3 \pmod 4$. In this case, $\mathfrak{o}=[1, \frac{1}{2}(1+\sqrt{-m_0})]$. A primitive form $Ax^2+2Bxy+Cy^2$ is properly or improperly primitive according as $(A, 2B, C)=1$ or 2. Both cases can be treated similarly as in case I:

(i) Case of properly primitive forms. We must put $R=[1, \sqrt{-m}]$, $\mathfrak{f}=2f\mathfrak{o}$. We then have $K_1=\dfrac{4f}{w}\displaystyle\prod_{p\mid 2f}\left(1-\frac{\chi(p)}{p}\right)$

(ii) Case of improperly primitive forms. In this case f must be odd. We must put $N(\alpha_1 x+\alpha_2 y)=\frac{1}{2}N\mathfrak{a}F(x, y)$, $R=[1, \frac{1}{2}(1+\sqrt{-m})]$, and $\mathfrak{f}=f\mathfrak{o}$. We then have

$$K_2=\begin{cases}0 & (\text{if } m>3,\ m \text{ even})\\ \dfrac{2f}{w}\displaystyle\prod_{p\mid f}\left(1-\frac{\chi(p)}{p}\right) & (\text{if } m>3,\ m \text{ odd})\\ 1 & (\text{if } m=3)\end{cases}$$

Then we have $H_1=(K_1+K_2)h$.

CALCULATION of H_2. To calculate the number of proper classes of quadratic forms, it is sufficient to consider reduced forms $Ax^2+2Bxy+Cy^2$, $|2B|\leqq A\leqq C$. A self conjugate form is equivalent to a reduced one for which $B=0$ or $A=C$ or $2B=A$. By applying a substitution $x=-y'$, $y=x'+y'$, to forms in the last case, we can unify the latter two cases. Hence we have two cases:

(i) Ax^2+Cy^2, $0<A\leqq C$, $(A, C)=1$, $AC=m$. There are 2^{t-1} such forms, if $m>1$; one form, if $m=1$.

(ii) $Ax^2+2Bxy+Ay^2$, $0<B<A$, $(A, B)=1$, $A^2-B^2=m$. There are

2^{t-1} such forms, if $m\equiv 1 \pmod 2$ and $m>1$ or $m\equiv 0 \pmod 8$; no form otherwise.

Since H_2 is a sum of the numbers in (i) and (ii), we have

$$H_2=\begin{cases} 2^t \text{ if } m \text{ is odd or } m\equiv 0 \pmod 8 \\ 2^{t-1} \text{ if } m\equiv 2, 4, 6 \pmod 8 . \end{cases}$$

§ 8. **Class number formulas.** We summarize our calculations in the following formulas for H. *Writing*

$$\psi(f)=f\prod_{p|f}\left(1-\frac{\chi(p)}{p}\right)$$

we have:

I. *If* $m_0\equiv 1 \pmod 4$, f *odd or* $f\equiv 0 \pmod 4$; *or* $m_0\equiv 2 \pmod 4$, f *even, then* $H=\frac{h}{w}\psi(f)$

II. *If* $m_0\equiv 1 \pmod 4$, $f=2f_0$, f_0 *odd*; *or* $m_0\equiv 2 \pmod 4$, f *odd, then* $H=\frac{h}{w}\psi(f)-2^{t-2}$

III. *If* $m_0\equiv 3 \pmod 4$, f *odd, then* $H=\frac{h}{w}(\psi(2f)+\psi(f))$

IV. *If* $m_0\equiv 3 \pmod 4$, $f\equiv 0 \pmod 4$, *then* $H=\frac{h}{w}\psi(2f)$

V. *If* $m_0\equiv 3 \pmod 4$, $f=2f_0$, f_0 *odd, then* $H=\frac{h}{w}\psi(2f)-2^{t-2}$

except when m *is* 1 *or* 3. *In cases that* m *is* 1 *and* 3, H *is* 0 *and* 1 *respectively.* ($m=f^2m_0$, m_0 *is square free*; w *is the number of units of the principal order* $\mathfrak{o}$; h *the number of ideal classes of* $\mathfrak{o}$; $\chi(p)$ *the Kronecker symbol for* $Q(\sqrt{-m_0})$; t *the number of prime factors of* m)

These formulas imply in particular that $H>0$ in cases I, III, IV. We now consider case II. Suppose first $m_0\equiv 1 \pmod 4$. We denote by t_0 the number of prime factors of $4m_0$; and by t_1 the number of prime factors of f_0 that do not divide m_0. Then 2^{t_0-1} is the number of ambiguous ideal classes of $\mathfrak{o}$, so that we have $2^{t_0-1}\mid h$. We can easily see that $2^{t_1}\mid\psi(f_0)$. We have $\psi(f)=2\psi(f_0)$, since $\chi(2)=0$. From these facts we know that H is zero if and only if $w=4$, $h=2^{t_0-1}$ and $\psi(f_0)=2^{t_1}$. These conditions mean that $m_0=f_0=1$. Suppose next $m_0\equiv 2 \pmod 4$. We denote by t_0 the number of prime factors of m_0; and by t_1 the number of prime factors of f that do not divide m_0. Noticing that $w=2$ in this case, we can see that $H=0$ if and only if $h=2^{t_0-1}$ and $\psi(f)=2^{t_1}$. The last equality holds if and only if $f=1$; or $f=3$ and $\chi(3)=1$. Finally we consider case V. We denote by t_0 the number of prime factors of m_0; and by t_1 the numbers of prime factors of f_0 that do not divide m_0. Noticing that $\chi(2)=-1$ for $Q(\sqrt{-3})$, we can see that $H=0$ if and only if $w=2(2-\chi(2))$, $h=2^{t_0-1}$ and $\psi(f_0)=2^{t_1}$.

Namely, $H=0$ if and only if $m_0=3$ and $f_0=1$; or $m_0>3$, $\chi(2)=1$ (i. e. $m_0\equiv -1 \pmod 8$), $h=2^{t_0-1}$ and $\psi(f_0)=2^{t_1}$. The last equality holds if and only if $f_0=1$; or $f_0=3$ and $\chi(3)=1$ (i. e. $m_0\equiv -1 \pmod 3$). Thus we have proved the following

THEOREM. *Let E and E' be two mutually isogenous elliptic curves whose rings of endomorphisms are isomorphic to the ring Z of rational integers. Then $E\times E'$ can not be a Jacobian variety if and only if the degree m of the basic homomorphism of E on E' is equal to one of the following integers:* (i) 1, 4, 12; (ii) f^2m_0 (m_0 *is square free*) *for which every ideal class of the principal order of $Q(\sqrt{-m_0})$ is ambiguous, and $f=1$, $m_0\equiv 2 \pmod 4$; $f=3$, $m_0\equiv 2 \pmod{12}$; $f=2$, $m_0\equiv -1 \pmod 8$; or $f=6$, $m_0\equiv -1 \pmod{24}$.*

On the other hand by virtue of a well known theorem of Siegel [6], we can easily see from the above formulas that H tends to infinity with m. In particular, there are only a finite number of values of m for which $E\times E'$ can not be a Jacobian variety.

Bibiliography

[1] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ. Hamburg (1941).

[2] T. Hayashida and M. Nishi, Existence of curves of genus two on a product of two elliptic curves, J. Math. Soc. Japan, Vol. 17, No. 1 (1965).

[3] G. B. Mathews, Theory of numbers, Chelsea, New York.

[4] M. Nishi, Some results on abelian varieties, Nat. Sci. Rep. Ochanomizu Univ. Vol. 9, No. 1 (1958).

[5] J. P. Serre, Faisceaux algébriques cohérent, Ann. of Math. Vol. 61 (1955).

[6] C. L. Siegel, Über die Classenzahl quadratischer Zahlkörper, Acta Arith. 1 (1935).

[7] A. Weil, Variétés abéliennes, Actualités Sci. Ind. (1948).

[8] A. Weil, Zum Beweis des Torellischen Satzes, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II (1957).