J. Math. Sci. Univ. Tokyo
14 (2007), 99–111.

The Hodge Rings of Abelian Varieties Associated to Certain Subsets of Finite Fields

By Fumio HAZAMA

Abstract. We construct a family of abelian varieties of CM-type such that the Hodge conjecture holds true for infinitely many members of it as well as their self-products. An intimate connection between the distribution of stably nondegenerate abelian varieties in the family and the coefficients of a certain modular form is revealed.

1. Introduction

The purpose of this paper is to give an example of a family of abelian varieties of CM-type such that the Hodge conjecture holds true for infinitely many members as well as their self-products. Originally the CM-types of the members emerge unexpectedly in the course of our study in [4] of counting functions of certain combinatorial objects attached to line arrangement. For any prime $p \geq 5$ and an integer $c \in [2, p-2] = \{n \in Z; 2 \leq n \leq p-2\}$, let $Z_{(p;c)}(x,y) = \sum_{(m,n)\in Z^2} x^{\max\{|m|,|cm+pn|\}} y^{|m|+|cm+pn|}$ and $W_{(p;c)}(x,y) = 1 + (Z_{(p;c)}(x,y) - 1)/2$. For any $a, b \in [1, p-1]$, let $\langle \frac{a}{b} \rangle_p \in [1, p-1]$ denote the unique integer such that $\langle \frac{a}{b} \rangle_p \equiv ab^{-1}$ in $\mathbf{F}_p$. In [loc.cit.], we obtain a formula which expresses $W_{(p;c)}(x,y)$ in the form

$$
\begin{aligned}
(1.1) \quad W_{(p;c)}(x,y) &= \sum_{0<r<p} \frac{X^r(Y^{\langle \frac{r}{c-1} \rangle_p} + Y^{\langle \frac{-cr}{c-1} \rangle_p} + Y^{\langle \frac{-cr}{c+1} \rangle_p} + Y^{\langle \frac{-r}{c+1} \rangle_p})}{(1-X^p)(1-Y^p)} \\
&\quad + \frac{(1+X^p)(1+Y^p)}{(1-X^p)(1-Y^p)},
\end{aligned}
$$

where $X = xy$, $Y = xy^2$. Let $T_{(p;c)} = \{\left\langle \frac{1}{c-1} \right\rangle_p, \left\langle \frac{-c}{c-1} \right\rangle_p, \left\langle \frac{-c}{c+1} \right\rangle_p, \left\langle \frac{-1}{c+1} \right\rangle_p\}$ and observe that the set of powers of Y in the summand on the right hand side consists of the orbit of $T_{(p;c)}$ under the natural action of $\mathbf{F}_p^*$. This

2000 *Mathematics Subject Classification.* 14C30, 14K22, 11G05.

observation leads us to the study of the abelian variety $A_{(p;c)}$ of CM-type attached to $T_{(p;c)}$. The main theorem (Theorem 3.5) shows that $A_{(p;c)}$ is stably nondegenerate in the sense of [2] whenever $p \equiv 3 \pmod 4$. As a result we see that every self-product $A^n_{(p;c)}$, $n \geq 1$, satisfies the Hodge conjecture. On the other hand, when $p \equiv 5 \pmod 8$, we establish a formula (Theorem 3.9) which counts the number of c for which $A_{(p;c)}$ is stably nondegenerate. The formula relates the number with the coefficient of the q-expansion of a certain modular form of conductor equal to 32.

The plan of this paper is as follows. In Section two we recall some results on the structure of the ring of Hodge cycles on abelian varieties of CM-type. In particular we recall the definition of stable nondegeneracy of an abelian variety, and a criterion for stable nondegeneracy given in [2] in terms of the dimension of the Hodge group. By applying the criterion to our abelian varieties of CM-type, we give a proof of the main theorem in Section three. Furthermore we find that there exists a close connection between the set of c for which $A_{(p;c)}$ is stably nondegenerate and the coefficients of a certain modular form of conductor 32.

2. Generality on the Hodge Rings of Abelian Varieties of CM-type

In this section, we recall some fundamental facts on the structure of the ring of Hodge cycles on abelian varieties of CM-type.

Let L be a galois CM-field of degree $2n$ with $Gal(L/\mathbf{Q}) \cong G = \{g_1, \cdots, g_n, g_1\rho, \cdots, g_n\rho\}$, where ρ denotes the complex conjugation. Let S be a CM-type for G so that $S \coprod S\rho = G$. Let A_S denote the abelian variety of CM-type associated to S (up to isogeny). When no confusion arises, we identify a subset X of G with the corresponding sum $\sum_{x \in X} x$ in the group ring $\mathbf{Q}[G]$. With this understood, we put $h_g = Sg - S\rho g \in \mathbf{Q}[G]$ for any $g \in G$. As a $\mathbf{Q}$-vector space, $\mathbf{Q}[G]$ is isomorphic to $\mathbf{Q}^{2n}$ through the numbering of the elements of G given above, so that we regard h_{g_i} as a row vector of length $2n$. We define the *Hodge matrix* H_S to be the n by $2n$ matrix, whose i-th row vector is h_{g_i}, $1 \leq i \leq n$. Then one knows that

$$\dim Hg(A_S) = \operatorname{rank} H_S,$$

where $Hg(A_S)$ denotes the Hodge group of A_S (see [2], [3]). In general the inequality $\dim Hg(A_S) \leq \dim A_S$ holds true for any S. When the equality

$\dim Hg(A_S) = \dim A_S$ holds, the abelian variety A_S is *stably nondegenerate* in the sense that the Hodge ring of A_S as well as those of its self-products are generated by the divisor classes, and in particular the Hodge conjecture holds for them ([2]). Therefore if we put $d(A_S) = \dim A_S - \dim Hg(A_S)$, called the *degeneracy of* A_S, then it gives us a rough index of the amount of nondivisorial Hodge cycles on A_S as well as A_S^n, $n \geq 1$. When the field L is an abelian number field, one can compute the degeneracy by using the character group $X(G)$ of G as follows. Let $X(G)^+$ (resp. $X(G)^-$) the set of even (resp. odd) characters of G. For any character $\chi \in X(G)$ and any element $\mathbf{v} = \sum_{g\in G} a_g g \in \mathbf{Q}[G]$, we define the character sum $\chi(\mathbf{v})$ by $\chi(\mathbf{v}) = \sum_{g\in G} a_g \chi(g) \in \mathbf{C}$. Then one has

$$\dim Hg(A_S) = \#\{\chi \in X(G)^-; \chi(S) \neq 0\}.$$

Therefore if we define the *annihilator* of S by $\operatorname{ann}_G^- S = \{\chi \in X(G)^-; \chi(S) = 0\}$, then we have $d(A_S) = \#(\operatorname{ann}_G^- S)$.

3. The Hodge Cycles on the Abelian Variety $A_{(p;c)}$

In this section we investigate the structure of the ring of Hodge cycles on the abelian variety $A_{(p;c)}$, in particular consider when it is stably nondegenerate.

The powers up to which Y is raised in the summand of the right hand side of (1.1) reminds us of certain types of abelian varieties of CM-type. To identify them more precisely, we introduce some notation. Let p be a prime ≥ 5. Let $H_p = \mathbf{F}_p^*$ and let K denote a CM-field with galois group $Gal(K/\mathbf{Q})$ isomorphic to $G_p = H_p \times \{\pm 1\}$, such that $(1, -1) \in G_p$ corresponds to the complex conjugation ρ. We regard H_p as a subgroup of G_p through the natural injection $H_p \to H_p \times \{1\} \subset G_p$. For any $c \in H_p - \{\pm 1\}$, let

$$T_{(p;c)} = \{(c-1)^{-1},\ -c(c-1)^{-1},\ -c(c+1)^{-1},\ -(c+1)^{-1}\} \subset H_p,$$

which corresponds to the set of powers in the summand of (1.1) for $r = 1$, and let

$$S_{(p;c)} = \{(a, 1); a \in T_{(p;c)}\} \cup \{(b, -1); b \in H_p - T_{(p;c)}\} \subset G_p.$$

Then the subset $S_{(p;c)}$ satisfies $G_p = S_{(p;c)} \coprod \rho S_{(p;c)}$ (disjoint union). Therefore $S_{(p;c)}$ is a CM-type, and we can associate to $S_{(p;c)}$ an abelian variety

$A_{(p;c)}$ of CM-type, which is of dimension $p-1$. First of all we check when $\#(T_{(p;c)}) < 4$.

PROPOSITION 3.1. *Suppose that* $c \in H_p - \{\pm 1\}$. *Then* $\#(T_{(p;c)}) < 4$ *if and only if* $c^2 = -1$, *and in that case* $T_{(p;c)} = \{(c-1)^{-1},\ c(1-c)^{-1}\}$. *In particular there exists an element* c *with* $c \in H_p - \{\pm 1\}$ *such that* $\#(T_{(p;c)}) < 4$ *if and only if* $p \equiv 1 \ (\mathrm{mod} 4)$.

PROOF. We name the elements of $T_{(p;c)}$ as $t_1 = (c-1)^{-1}$, $t_2 = -c(c-1)^{-1}$, $t_3 = -c(c+1)^{-1}$, $t_4 = -(c+1)^{-1}$, and consider when a pair of them coincides. Suppose that $t_1 = t_2$. This occurs when $(c-1)^{-1} = -c(c-1)^{-1}$, which is equivalent to $c = -1$. This is not the case by our assumption. The other five cases can be treated similarly and we have the following:

$t_1 = t_3 \Leftrightarrow (c-1)^{-1} = -c(c+1)^{-1} \Leftrightarrow c^2 = -1.$
$t_1 = t_4 \Leftrightarrow (c-1)^{-1} = -(c+1)^{-1} \Leftrightarrow c = 0,$ which is not the case.
$t_2 = t_3 \Leftrightarrow -c(c-1)^{-1} = -c(c+1)^{-1} \Leftrightarrow 2 = 0,$ which is not the case.
$t_2 = t_4 \Leftrightarrow -c(c-1)^{-1} = -(c+1)^{-1} \Leftrightarrow c^2 = -1.$
$t_3 = t_4 \Leftrightarrow -c(c+1)^{-1} = -(c+1)^{-1} \Leftrightarrow c = 1,$ which is not the case.

This completes the proof of Proposition 3.1. □

The following proposition shows that the abelian varieties $A_{(p;c)}$ are always absolutely simple except when $p = 5$.

PROPOSITION 3.2. *When* $p \geq 7$, *the abelian variety* $A_{(p;c)}$ *is absolutely simple for any* $c \in H_p - \{\pm 1\}$. *When* $p = 5$, *then the four dimensional abelian varieties* $A_{(5;2)}$ *and* $A_{(5;3)}$ *are isogenous to the self-product of an abelian surfaces of CM-type.*

PROOF. One knows that the absolute simplicity of $A_{(p;c)}$is equivalent to the equality

$$\{s \in G_p; sS_{(p;c)} = S_{(p;c)}\} = \{(1,1)\}$$

(see [5, Ch.8, Proposition 26]). Suppose that $p \geq 7$. Since we have the equalities

$$\#((t,-1)S_{(p;c)} \cap H_p) = \#(H_p - T_{(p;c)}) = p - 1 - \#T_{(p;c)},$$
$$\#(S_{(p;c)} \cap H_p) = \#T_{(p;c)},$$

and $\#T_{(p;c)} \neq p-1-\#T_{(p;c)}$ by Proposition 3.1, we see that $(t,-1)S_{(p;c)} \neq S_{(p;c)}$ for any $t \in H_p$. On the other hand if $(t,1)S_{(p;c)} = S_{(p;c)}$, then we must have

$$tT_{(p;c)} = T_{(p;c)}. \tag{3.1}$$

Note that if we add the elements of $T_{(p;c)}$ in $\mathbf{F}_p$, then the total, which we denote by $\sum T_{(p;c)} \in \mathbf{F}_p$, is equal to

$$\begin{aligned}&(c-1)^{-1} + (-c)(c-1)^{-1} + (-c)(c+1)^{-1} + (-1)(c+1)^{-1}\\ &= (1-c)(c-1)^{-1} + (-c-1)(c+1)^{-1},\end{aligned}$$

which is equal to -2 if $\#T_{(p;c)} = 4$, or equal to -1 if $\#T_{(p;c)} = 2$. In any case we have $\sum T_{(p;c)} \neq 0$ and hence (3.1) implies that $(t-1)\sum T_{(p;c)} = 0$, and hence $t = 1$. This proves our proposition in the case $p \geq 7$. When $p = 5$, the only possible value for c is 2 or 3, and we have

$$\begin{aligned}&T_{(5;2)} = T_{(5;3)} = \{1,3\} \subset H_5,\\ &S_{(5;2)} = S_{(5;3)} = \{(1,1),(3,1),(2,-1),(4,-1)\} \subset G_5.\end{aligned}$$

Therefore the Hodge matrix $H_{S_{(5;2)}} = H_{S_{(5;3)}}$ is given by

$$H_{S_{(5;2)}} = \begin{pmatrix} 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\ -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \end{pmatrix},$$

where we name the elements of G_p as $g_1 = (1,1)$, $g_2 = (2,1)$, $g_3 = (3,1)$, $g_4 = (4,1)$. The rank of $H_{S_{(5;2)}}$ is readily seen to be equal to two, hence by a general fact on the Hodge group (see [2], [3]) we see that $A_{(5;2)}$ as well as $A_{(5;3)}$ is isogenous to the self-product A^2 of an abelian surfaces A of CM-type. This completes the proof of Proposition 3.2. $\square$

Since any abelian surface of CM-type is known to be stably nondegenerate ([2]), we assume in the rest of the paper that $p \geq 7$. As is recalled in the previous section, the structure of the Hodge rings of the self-products of $A^n_{(p;c)}$, $n \geq 1$, is controlled by the annihilator $\mathrm{ann}^-_{G_p} S_{(p;c)} \subset X(G_p)^-$. Furthermore the following simple observation enables us to consider everything in H_p. Let $\Phi : X(G_p)^- \to X(H_p)$ and $\Psi : X(H_p) \to X(G_p)^-$ be defined by

$$\Phi(\chi) = \chi\,|_{H_p} \tag{3.2}$$

$$\Psi(\theta)(a,\varepsilon) = \begin{cases} \theta(a), & if\ \varepsilon = 1, \\ -\theta(a), & if\ \varepsilon = -1, \end{cases} \quad \text{for any } (a,\varepsilon) \in G_p. \tag{3.3}$$

One can check that these are inverses to each other. Moreover for any CM-type $S \subset G_p$ we define $S' \in \mathbf{Z}[H_p]$ by $S' = \sum_{(a,1)\in S} a - \sum_{(b,-1)\in S} b$. Then, we have

$$\chi(S) = \Phi(\chi)(S') \text{ for any } \chi \in X(G_p)^-, \tag{3.4.a}$$

$$\Psi(\theta)(S) = \theta(S') \text{ for any } \theta \in X(H_p). \tag{3.4.b}$$

In particular for the trivial character $\mathbf{1} \in X(H_p)$, we have

$$\Psi(\mathbf{1})(S_{(p;c)}) = \mathbf{1}(S'_{(p;c)}) = \#T_{(p;c)} - (p-1-\#T_{(p;c)}) = 2(\#T_{(p;c)}) - p + 1.$$

Since we have assumed that $p \geq 7$ and $\#T_{(p;c)} = 4$ or 2 by Proposition 3.1, the right hand side cannot vanish. Therefore $\Psi(\mathbf{1}) \notin \mathrm{ann}^-_{G_p} S_{(p;c)}$. Furthermore, since $\theta(H_p) = 0$ for any nontrivial character $\theta \in X(H_p)$, we see that for any $\theta \in X(H_p) - \{\mathbf{1}\}$ we have

$$\begin{aligned} \Psi(\theta)(S_{(p;c)}) &= \theta(S'_{(p;c)}) = \theta(T_{(p;c)}) - \theta(H_p - T_{(p;c)}) \\ &= 2\theta(T_{(p;c)}) - \theta(H_p) = 2\theta(T_{(p;c)}). \end{aligned}$$

Thus we obtain the following.

PROPOSITION 3.3. *Let* $\mathrm{ann}_{H_p} T_{(p;c)} = \{\theta \in X(H_p); \theta(T_{(p;c)}) = 0\}$. *Then we have* $\mathrm{ann}^-_{G_p} S_{(p;c)} = \Psi(\mathrm{ann}_{H_p} T_{(p;c)})$. *In particular,* $d(A_{(p;c)}) = \#(\mathrm{ann}_{H_p} T_{(p;c)})$.

Therefore we are reduced to the investigation of the set $\mathrm{ann}_{H_p} T_{(p;c)}$. The next proposition provides us with a criterion for vanishing of the character sum $\theta(T_{(p;c)})$.

PROPOSITION 3.4. *For a character* $\theta \in X(H_p)$, *the character sum* $\theta(T_{(p;c)})$ *vanishes if and only if one of the following conditions holds:*

(i) $\theta \in X(H_p)^+$ *and* $\theta(c) = -1$,

(ii) $\theta \in X(H_p)^+$ *and* $\theta((c+1)(c-1)^{-1}) = -1$,

(iii) $\theta \in X(H_p)^-$ *and* $\theta(c) = \theta((c+1)(c-1)^{-1}) = \pm\sqrt{-1}$.

PROOF. The character sum $\theta(T_{(p;c)})$ is computed to be

$$\begin{aligned}\theta(T_{(p;c)}) &= \theta\left((c-1)^{-1}\right) + \theta\left(-c(c-1)^{-1}\right) + \theta\left(-c(c+1)^{-1}\right)\\ &\quad + \theta\left(-(c+1)^{-1}\right)\\ &= \theta\,(c-1)^{-1} + \theta\,(-c)\,\theta\,(c-1)^{-1} + \theta\,(-c)\,\theta\,(c+1)^{-1}\\ &\quad + \theta\,(-1)\,\theta\,(c+1)^{-1}.\end{aligned}$$

Hence if $\theta \in X(H_p)^+$, then we have

$$\begin{aligned}\theta(T_{(p;c)}) &= \theta\,(c-1)^{-1} + \theta\,(c)\,\theta\,(c-1)^{-1} + \theta\,(c)\,\theta\,(c+1)^{-1} + \theta\,(c+1)^{-1}\\ &= (1+\theta\,(c))(\theta\,(c-1)^{-1} + \theta\,(c+1)^{-1})\\ &= (1+\theta(c))(1+\theta\left((c+1)(c-1)^{-1}\right))\theta(c+1)^{-1}.\end{aligned}$$

Therefore we see that $\theta(T_{(p;c)}) = 0$ if and only if $\theta(c) = -1$ or $\theta((c+1)(c-1)^{-1}) = -1$. On the other hand if $\theta \in X(H_p)^-$, then we have

$$\begin{aligned}\theta(T_{(p;c)}) &= \theta\,(c-1)^{-1} - \theta\,(c)\,\theta\,(c-1)^{-1} - \theta\,(c)\,\theta\,(c+1)^{-1} - \theta\,(c+1)^{-1}\\ &= (1-\theta\,(c))\theta\,(c-1)^{-1} - (1+\theta\,(c))\theta\,(c+1)^{-1}.\end{aligned}$$

Note that if $\theta(c) = 1$, then $\theta(T_{(p;c)}) = -2\theta\,(c+1)^{-1}$, which cannot vanish. Therefore we see that $\theta(T_{(p;c)}) = 0$ if and only if

$$\frac{\theta\,(c+1)}{\theta\,(c-1)} = \frac{1+\theta\,(c)}{1-\theta\,(c)}. \tag{3.5}$$

Since the absolute value of the left hand side is equal to one, we have

$$|1+\theta\,(c)| = |1-\theta\,(c)|,$$

which implies that $\theta(c)$ is purely imaginary. Hence $\theta\,(c) = \pm\sqrt{-1}$, and in this case, we have

$$\frac{1+\theta\,(c)}{1-\theta\,(c)} = \frac{1\pm\sqrt{-1}}{1\mp\sqrt{-1}} = \pm\sqrt{-1}.$$

This implies by (3.5) that $\theta(c) = \theta((c+1)/(c-1)^{-1}) = \pm\sqrt{-1}$. Thus we complete the proof. $\square$

By using this proposition we prove one of the main results in this paper:

THEOREM 3.5. *When $p \equiv 3 \pmod 4$, the abelian variety $A_{(p;c)}$ is stably nondegenerate for any $c \in H_p - \{\pm 1\}$. In particular the Hodge conjecture holds true for $A^n_{(p;c)}$, $n \geq 1$.*

PROOF. Let $p = 4k+3$ for some positive integer k. For any positive integer m, let $\mu_m \subset \mathbf{C}^*$ denote the group of m-th roots of unity. If $\theta \in X(H_p)^+$, then we have $\theta(d) \in \mu_{(p-1)/2} = \mu_{2k+1}$ for any $d \in H_p$. Therefore there is no $c \in H_p - \{\pm 1\}$ such that $\theta(c) = -1$ or $\theta((c+1)(c-1)^{-1}) = -1$. Hence Proposition 3.4 implies that $\theta(T_{(p;c)}) \neq 0$ for any $\theta \in X(H_p)^+$. On the other hand, if $\theta \in X(H_p)^-$, then $\theta(d) \in \mu_{p-1} = \mu_{4k+2}$, and the element $\sqrt{-1}$, which is of order four, cannot belong to μ_{4k+2}. Hence Proposition 3.4 implies again that $\theta(T_{(p;c)}) \neq 0$ for any $\theta \in X(H_p)^-$. This completes the proof of Theorem 3.5. $\square$

Now we proceed to the study of the case when $p \equiv 1 \pmod 4$. We begin with some examples. Let us fix a $(p-1)$-th root of unity ζ_{p-1}. For a primitive root r modulo p, let $\theta^a_r \in X(H_p)$, $0 \leq a \leq p-2$, be defined by $\theta^a_r(r) = \zeta^a_{p-1}$, and let

$$\mathrm{Ind}(\mathrm{ann}_{H_p} T_{(p;c)}) = \{a \in [0, p-2]; \theta^a_r \in \mathrm{ann}_{H_p} T_{(p;c)}\}.$$

One can see that this set does not depend on the choice of r as follows. Let φ_k, $k \in (\mathbf{Z}/(p-1)\mathbf{Z})^*$, denote the element of the galois group $Gal(\mathbf{Q}(\zeta_{p-1})/\mathbf{Q})$ defined by $\varphi_k(\zeta_{p-1}) = \zeta^k_{p-1}$. Let $\bar{k}$ denote the inverse of $k \in (\mathbf{Z}/(p-1)\mathbf{Z})^*$. Then we have $\varphi_k(\theta^a_r(r^j)) = \zeta^{akj}_{p-1} = \theta^a_{r^{\bar{k}}}(r^{\bar{k}kj}) = \theta^a_{r^{\bar{k}}}(r^j)$. Therefore $\mathrm{Ind}(\mathrm{ann}_{H_p} T_{(p;c)})$ does not depend on the choice of r. The following table shows $T_{(p;c)}$ and $\mathrm{Ind}(\mathrm{ann}_{H_p} T_{(p;c)})$ for small values of p and $c \in H_p - \{\pm 1\}$:

As one can see from this table, the situation is rather mysterious. We can, however, obtain some positive results when $p \equiv 5 \pmod 8$.

THEOREM 3.6. *Suppose that $p \equiv 5 \pmod 8$. For any $c \in H_p - \{\pm 1\}$, the abelian variety $A_{(p;c)}$ is stably nondegenerate if and only if c satisfies the*

Table 1.

p	c	$T_{(p;c)}$	$\mathrm{Ind}(\mathrm{ann}_{H_p} T_{(p;c)})$	$d(A_{(p;c)})$
13	2, 6, 7, 11	$\{1,4,8,11\}$	$\{6\}$	1
	3, 4, 9, 10	$\{3,5,7,9\}$	$\{6\}$	1
	5, 8	$\{2,10\}$	$\{2,6,10\}$	3
17	2, 8, 9, 15	$\{1,5,11,15\}$	$\{4,8,12\}$	3
	3, 6, 11, 14	$\{4,7,9,12\}$	$\{4,8,12\}$	3
	5, 7, 10, 12	$\{2,3,13,14\}$	$\{8\}$	1
	4, 13	$\{6,10\}$	$\{2,6,10,14\}$	4
29	2, 14, 15, 27	$\{1,9,19,27\}$	$\{7,14,21\}$	3
	3, 10, 19, 26	$\{7,13,15,21\}$	$\{7,14,21\}$	3
	4, 7, 22, 25	$\{5,10,18,23\}$	$\{14\}$	1
	5, 6, 23, 24	$\{4,6,22,24\}$	ϕ	0
	9, 13, 16, 20	$\{2,11,17,26\}$	ϕ	0
	8, 11, 18, 21	$\{3,12,16,25\}$	$\{14\}$	1
	12, 17	$\{8,20\}$	$\{2,6,10,14,18,22,26\}$	7
37	2, 18, 19, 35	$\{1,12,24,35\}$	$\{18\}$	1
	3, 12, 25, 34	$\{9,17,19,27\}$	$\{18\}$	1
	4, 9, 28, 33	$\{11,14,22,25\}$	$\{6,18,30\}$	3
	5, 15, 22, 32	$\{6,8,28,30\}$	$\{18\}$	1
	7, 16, 21, 30	$\{5,13,23,31\}$	ϕ	0
	8, 14, 23, 29	$\{4,16,20,32\}$	$\{6,18,30\}$	3
	10, 11, 26, 27	$\{3,10,26,33\}$	ϕ	0
	13, 17, 20, 24	$\{2,7,29,34\}$	$\{18\}$	1
	6, 31	$\{15,21\}$	$\{2,6,10,14,18,22,26,30,34\}$	9

condition

$$\left(\frac{c}{p}\right) = 1,\ \left(\frac{(c-1)(c+1)}{p}\right) = 1, \tag{3.6}$$

where $\left(\frac{\bullet}{p}\right)$ *denotes the Legendre symbol.*

PROOF. Let $p = 8k+5$ and fix a primitive root r modulo p. First we prove the only-if-part. Suppose that $c \in H_p - \{\pm 1\}$ is a quadratic non-residue modulo p. Then there exists an integer i such that $c = r^{2i+1}$. Then for the even character $\theta_r^{(p-1)/2} = \theta_r^{4k+2}$, we have $\theta_r^{4k+2}(c) = \zeta_{p-1}^{(4k+2)(2i+1)} = \zeta_{8k+4}^{(8k+4)i+(4k+2)} = \zeta_{8k+4}^{4k+2} = -1$. Therefore by Proposition 3.4, (i), the character sum $\theta_r^{4k+2}(T_{(p;c)})$ vanishes. On the other hand, if $(c-1)(c+1)$ is a quadratic nonresidue modulo p, then there exists an integer j such that $(c+1)(c-1)^{-1} = r^{2j+1}$. Hence we have $\theta_r^{4k+2}((c+1)(c-1)^{-1}) = -1$ and the character sum $\theta_r^{4k+2}(T_{(p;c)})$ vanishes by Proposition 3.4, (ii). In any case the negation of the condition (3.6) implies the existence of a character in $\mathrm{ann}_{H_p} T_{(p;c)}$, which proves the only-if-part by Proposition 3.3. Next we prove the if-part. By the assumption there exists a pair of integers i, j such that $c = r^{2i}$ and $(c+1)(c-1)^{-1} = r^{2j}$. Every even character θ is expressed as $\theta = \theta_r^{2\ell}$ with $0 \le \ell \le (p-3)/2 = 4k+1$. The condition $\theta_r^{2\ell}(c) = -1$ in Proposition 3.4, (i) is translated into $\zeta_{p-1}^{4\ell i} = \zeta_{p-1}^{(p-1)/2}$, which is equivalent to the congruence $4\ell i \equiv 4k+2 \pmod{8k+4}$, which is impossible. Similarly the condition $\theta_r^{2\ell}((c+1)(c-1)^{-1}) = -1$ in Proposition 3.4, (ii) cannot hold. Furthermore for any odd character $\theta_r^{2\ell+1}$, the condition $\theta_r^{2\ell+1}(c) = \pm\sqrt{-1}$ in Proposition 3.4, (iii), is expressed as $\zeta_{p-1}^{(2\ell+1)\cdot 2i} = \pm\zeta_{p-1}^{(p-1)/4}$. This is equivalent to the congruence $2(2\ell+1)i \equiv 2k+1$ *or* $6k+3 (\mathrm{mod}\ 8k+4)$, which is also impossible. This completes the proof of Theorem 3.6. □

Thus we are led naturally to the following problems:

(P.1) Does there exist an element $c \in H_p - \{\pm 1\}$ which satisfies the condition (3.6)?

(P.2) If so, how many elements in $H_p - \{\pm 1\}$ satisfy (i)?

In what follows we solve both problems by appealing to the theory of elliptic curves. Suppose that $c \in H_p - \{\pm 1\}$ satisfies (3.6). Then there exist $d, e \in \mathbf{F}_p^*$ such that $c = d^2$ and $(c+1)(c-1) = e^2$. By eliminating c, we obtain the equation

$$C : e^2 = d^4 - 1, \tag{3.7}$$

which defines an elliptic curve. We can find its Weierstrass form in the standard way (see [1], for example). Put $T = e + d^2$, then the equation (3.7) implies that $e - d^2 = -1/(e+d^2) = -1/T$. Subtracting these, we have $2d^2 = T + 1/T$, and multiplying the both sides by 2^3T^2 we obtain $(4dT)^2 = (2T)^3 + 4 \cdot 2T$. Letting $x = 2T$, $y = 4dT$, we arrive at the Weierstrass form

$$E : y^2 = x^3 + 4x.$$

Tracing the coordinate changes, we see that a point $(x, y) \in E$ goes to the point $(d, e) = (y/(2x),\ (x^2-4)/(4x)) \in C$, which gives rise to the value $c = d^2 = y^2/(2x)^2 = (x^3+4x)/(4x^2) = (x^2+4)/(4x)$. Therefore $c \in H_p - \{\pm 1\}$ if and only if $x \in \mathbf{F}_p - \{0, \pm 2, \pm 2\sqrt{-1}\}$. (Note that -1 is quadratic residue since $p \equiv 1 \pmod 4$.) Thus we obtain the following.

PROPOSITION 3.7. *An element $c \in H_p - \{\pm 1\}$ satisfies the condition (3.6) in Theorem 3.6 if and only if it is expressed as $c = (x^2+4)/(4x)$ where x is the x-coordinate of an $\mathbf{F}_p$-rational point of the elliptic curve $E : y^2 = x^3 + 4x$ with $x \in \mathbf{F}_p - \{0, \pm 2, \pm 2\sqrt{-1}\}$.*

Furthermore we can show the following.

PROPOSITION 3.8. *Let sq_p denote the number of elements $c \in H_p - \{\pm 1\}$ such that the condition (3.6) in Theorem 3.6 holds for c. Then we have*

$$sq_p = \frac{\#(E(\mathbf{F}_p)) - 8}{4}. \tag{3.8}$$

PROOF. Let $\pi_1 : E - \{\mathcal{O}\} \to \mathbf{A}^1$ be the natural projection defined by $\pi_1(x,y) = x$, where $\mathcal{O}$ denotes the origin of E. Furthermore let $\pi_2 : \mathbf{A}^1 - \{0\} \to \mathbf{A}^1$ denote the map defined by $\pi_2(x) = (x^2+4)/(4x)$. Since for a given $c \in \mathbf{A}^1$, the condition $\pi_2(x) = c$ gives rise to a quadratic equation $x^2 - 4cx + 4 = 0$ of discriminant $16c^2 - 16 = 16(c-1)(c+1)$, the map π_2 is 2 to 1 everywhere when restricted to $\pi_2^{-1}(\mathbf{A}^1 - \{\pm 1\})$. Note that $\pi_2^{-1}(\{\pm 1\}) = \{\pm 2\}$, $\pi_2^{-1}(\{0\}) = \{\pm 2\sqrt{-1}\}$. Moreover the map π_1 is 2 to 1 everywhere when restricted to $\pi_1^{-1}(\mathbf{A}^1 - \{0, \pm 2\sqrt{-1}\})$ and $\pi_1^{-1}(\{0, \pm 2\sqrt{-1}\}) = \{(0,0), (\pm 2\sqrt{-1}, 0)\}$, $\pi_1^{-1}(\{\pm 2\}) = \{(2, \pm 4), (-2, \pm 4)\}$. Therefore the composed map $\pi_2 \circ \pi_1$ defines an everywhere 4-to-1 surjective map from $E - \{\mathcal{O}, (0,0), (\pm 2\sqrt{-1}, 0), (2, \pm 4), (-2, \pm 4)\}$ to $\mathbf{A}^1 - \{0, \pm 1\}$. Note that Proposition 3.7 implies the equality

$$sq_p = \#(\pi_2 \circ \pi_1(E(\mathbf{F}_p) - \{\mathcal{O}, (0,0), (\pm 2\sqrt{-1}, 0), (2, \pm 4), (-2, \pm 4)\})),$$

and hence the argument above implies that $4 sq_p = \#(E(\mathbf{F}_p)) - 8$. This completes the proof of Proposition 3.8. □

Thus our final task is to find $\#(E(\mathbf{F}_p))$. For this there is a well-known bound $|\#(E(\mathbf{F}_p)) - (p+1)| \leq 2\sqrt{p}$. From this follows that

$$\#(E(\mathbf{F}_p)) \geq p + 1 - 2\sqrt{p} = (\sqrt{p} - 1)^2,$$

and hence if $p \geq 17$, then the formula (3.8) implies that $sq_p > 0$. This solves the problem (P.1) when $p \geq 17$. On the contrary, if $p = 5, 13$, then there are no c which satisfies the condition (3.6), as is seen by (3.8) or the Table 2 below.

In order to solve the problem (P.2), we employ the modular parameterization of the elliptic curve E which has conductor equal to 32. It is known to be associated with the cusp form $f = \eta(4z)^2\eta(8z)^2$, whose q-expansion can be computed easily as follows:

$$\begin{aligned} f \;=\; & q - 2q^5 - 3q^9 + 6q^{13} + 2q^{17} - q^{25} - 10q^{29} - 2q^{37} + 10q^{41} + 6q^{45} \\ & - 7q^{49} + 14q^{53} - 10q^{61} - 12q^{65} - 6q^{73} + 9q^{81} - 4q^{85} + 10q^{89} \\ & + 18q^{97} - 2q^{101} + 6q^{109} + O(q^{113}). \end{aligned}$$

Therefore if we put $f = \sum_{n \geq 0} a_n q^n$, then we have $a_p = p + 1 - \#(E(\mathbf{F}_p))$ for any prime p. Thus we obtain the following.

THEOREM 3.9. *Notation being as above, we have* $sq_p = (p - a_p - 7)/4$.

Some examples of the values of a_p, sq_p and the set of c satisfying the condition (i) in Theorem 3.6 are given below:

Table 2.

p	a_p	sq_p	the set of c
5	-2	0	ϕ
13	6	0	ϕ
29	-10	8	$\{5, 6, 9, 13, 16, 20, 23, 24\}$
37	-2	8	$\{7, 10, 11, 16, 21, 26, 27, 30\}$
53	14	8	$\{4, 10, 13, 16, 37, 40, 43, 49\}$
61	-10	16	$\{4, 9, 13, 14, 15, 22, 25, 27, 34, 36, 39, 46, 47, 48, 52, 57\}$
101	-2	24	$\{5, 9, 20, 21, 22, 23, 24, 33, 43, 45, 47, 49,$ $52, 54, 56, 58, 68, 77, 78, 79, 80, 81, 92, 96\}$
109	6	24	$\{4, 7, 9, 12, 21, 26, 27, 28, 31, 35, 38, 43,$ $66, 71, 74, 78, 81, 82, 83, 88, 97, 100, 102, 105\}$

References

[1] Cassels, J. W. S., *Lectures on Elliptic Curves*. LMS Student Texts, Cambridge University Press, 1991.

[2] Hazama, F., Algebraic cycles on certain Abelian varieties and powers of special surfaces, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **31** (1984), 487–520.

[3] Hazama, F., Hodge cycles on abelian varieties of S_n-type, J. Alg. Geom. **9** (2000), 711–753.

[4] Hazama, F., On HW-counting functions associated to certain line arrangements (preprint).

[5] Shimura, G. and Y. Taniyama, Complex multiplication of abelian varieties and its applications to number theory, Publ. Math. Soc. Japan, No. 6, 1961.

(Received July 24, 2006)
(Revised February 15, 2007)

Department of Natural Sciences
College of Science and Engineering
Tokyo Denki University
Hatoyama, Saitama 350-0394
JAPAN