TOKYO J. MATH.
VOL. 31, NO. 1, 2008

Counting Points of the Curve $y^2 = x^{12} + a$ over a Finite Field

Yasuhiro NIITSUMA

Chuo University

(Communicated by S. Miyoshi)

Abstract. We give explicit formulas of the number of rational points and those of the congruence zeta functions for the hyperelliptic curves over a finite field defined by affine equations $y^2 = x^6 + a$, $y^2 = x^{12} + a$ and $y^2 = x(x^6 + a)$.

Introduction

It is an interesting problem to count rational points of a non-singular projective curve over a finite field and those of the Jacobian variety. In [3], Buhler and Koblitz proposed a method to give explicit formulas for the number of rational points on the Jacobian variety of the hyperelliptic curve over a finite field defined by an affine equation $\alpha y^2 + y = \beta x^n$ for an odd prime number n, considering applications to cryptography. It is a key to their method to express the congruence zeta function in terms of Jacobi sums. In [5] and [6], Kawazoe and Takahashi gave explicit formulas for the congruence zeta function of the hyperelliptic curve over a finite field defined by an affine equation $y^2 = x^n + ax$ in the cases where $n = 5, 7, 9$. Recently, Ozaki [8] gave explicit formulas for the number of rational points and for the congruence zeta function of the non-singular projective curve over a finite field defined by an affine equation $y^4 = x^3 + a$.

In this article, we give explicit formulas of the number of rational points and those of the congruence zeta functions for the hyperelliptic curves over a finite field defined by affine equations

$$\begin{array}{ll} y^2 = x^6 + a & \text{(Proposition 2.1 and Corollary 2.8)} \\ y^2 = x^{12} + a & \text{(Proposition 3.1 and Theorem 4.2)} \\ y^2 = x(x^6 + a) & \text{(Proposition 5.1)} \end{array}$$

by determining Jacobi sums.

The point in the argument is to consider the coverings of hyperelliptic curves as follows:

Received July 28, 2006

Partially supported by The Research on Security and Reliability in Electronic Society, Chuo University 21st Century COE Program.

2000 *Mathematics Subject Classification*: 11G20 (primary), 14G10, 11L05 (secondary).

$$\begin{tikzcd}
& Y : y^2 = x^{12} + a \arrow[ddl] \arrow[dr] \arrow[drrr] & & & \\
& & X : y^2 = x^6 + a \arrow[ddl] \arrow[dr] & & \tilde{X} : y^2 = x^7 + ax \\
\tilde{E} : y^2 = x^4 + a \arrow[dr] & & & E : y^2 = x^3 + a & \\
& Q : y^2 = x^2 + a & & &
\end{tikzcd}$$

Now we explain in a typical case the argument of obtaining the formulas.

Let p be a prime number such that $p \equiv 1 \mod 12$. Then there exist uniquely a prime element $\pi = A + B\sqrt{-3}$ in the ring of Eisenstein integers and a prime element $\rho = C + D\sqrt{-1}$ in the ring of Gauss integers, where $A \equiv 1 \mod 3$, $B > 0$, $C \equiv 1 \mod 4$ and $D > 0$. Let χ denote the multiplicative character of the finite field $\mathbf{F}_p$ of order 12 defined by $\alpha \mapsto \left(\frac{\alpha}{\pi,\, \rho}\right)_{12}$. Then, by applying a theorem of Davenport-Hasse to the curves listed above, we obtain:

$$\begin{aligned}
\#E(\mathbf{F}_p) - (p+1) &= \mathrm{Tr}_{\mathbf{Q}(e^{2\pi i/3})/\mathbf{Q}}(\chi^{10}(a)J(\chi^4, \chi^6))\,, \\
\#\tilde{E}(\mathbf{F}_p) - (p+1) &= \mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}(\chi(-1)\chi^9(a)J(\chi^3, \chi^6))\,, \\
\#X(\mathbf{F}_p) - \#E(\mathbf{F}_p) &= \mathrm{Tr}_{\mathbf{Q}(e^{\pi i/3})/\mathbf{Q}}(\chi^8(a)J(\chi^2, \chi^6))
\end{aligned}$$

and

$$\begin{aligned}
\#Y(\mathbf{F}_p) - \#X(\mathbf{F}_p) = {} & \mathrm{Tr}_{\mathbf{Q}(e^{\pi i/6})/\mathbf{Q}}(\chi(-1)\chi^7(a)J(\chi, \chi^6)) \\
& + \mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}(\chi(-1)\chi^9(a)J(\chi^3, \chi^6))\,.
\end{aligned}$$

(For the notations, see the section 1.) Hence it remains to determine the Jacobi sums

$$J(\chi^4, \chi^6)\,, \quad J(\chi^3, \chi^6)\,, \quad J(\chi^2, \chi^6)\,, \quad J(\chi, \chi^6)\,.$$

It is crucial to restrict the possibilities of Jacobi sums in our cases, up to the multiplication by a power root of unity, with help of Stickelberger's theorem for Jacobi sums. At last we arrive at the main result, analyzing the trace of Jacobi sums.

Hereafter we explain the plan of the article in the typical case stated above.

In the section 1, after reviewing the definition of power residue symbols and Jacobi sums, we mention a theorem due to Stickelberger for Jacobi sums and a result due to Davenport-Hasse [4] on the congruence zeta function of the non-singular projective curve defined by an affine equation $ax^m + by^n = c$ over a finite field. We conclude the section by recalling the results on the Jacobi sums:

$$J(\chi^4, \chi^6) = -(A + B\sqrt{-3})$$

and

$$\chi(-1)J(\chi^3, \chi^6) = -(C + D\sqrt{-1})\,.$$

In the section 2, we determine the Jacobi sum $J(\chi^2, \chi^6)$. By considering the double covering $X \to E$ defined by $(x, y) \mapsto (x^2, y)$, we prove an important congruence

$$\mathrm{Tr}_{\mathbf{Q}(e^{\pi i/3})/\mathbf{Q}}(\chi(-1)J(\chi^2, \chi^6)) \equiv -2 \mod 6\,,$$

from which we obtain

$$\chi(-1)J(\chi^2, \chi^6) = -(A + B\sqrt{-3})\,.$$

The congruence zeta function of the hyperelliptic curve X over the finite field $\mathbf{F}_p$ is deduced from the result.

In the section 3, we determine the Jacobi sum $J(\chi, \chi^6)$. By considering the double covering $Y \to X$ defined by $(x, y) \mapsto (x^2, y)$, we prove an important congruecnce

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}\big(\chi(-1)J(\chi, \chi^6)\big) + \mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}\big(\chi^3(-1)J(\chi^3, \chi^6)\big) \equiv -6 \mod 24\,,$$

from which we obtain

$$\chi(-1)J(\chi, \chi^6) = \begin{cases} -\rho & \text{if } C \not\equiv 0 \mod 3\,, \\ \rho & \text{if } C \equiv 0 \mod 3\,. \end{cases}$$

In the section 4, we determine the congruence zeta function of the hyperelliptic curve defined by the affine equation $y^2 = x^{12} + a$. In the case where $p \not\equiv 1 \mod 12$, it is crucial to determine Jacobi sums over a quadratic extension field.

In the section 5, as a corollary of the theorem in the section 4, we obtain explicit formulas for the congruence zeta function of the hyperelliptic curve over a finite field defined by the affine equation $y^2 = x(x^6 + a)$.

It should be mentioned that some of our results can be deduced from the assertions mentioned in Berndt, Evans and Williams [2, Chapter 3]. We adopt here a method emphasizing relations between the Jacobi sums and the hyperelliptic curves.

ACKNOWLEDGMENT. The author expresses his sincere thanks to Professor Noriyuki Suwa for his advice and suggestion. He has learned much from his lecture in the winter semester 2004, getting materials of the section 1. Furthermore he is very grateful to the referee for his careful reading and his advice to improve the presentation.

CONTENTS

NOTATION

Throughout the article, p denotes a prime number and q a power of p.
$\mathbf{F}_q$: the finite field of order q
$\mathbf{F}_q^\times$: the multiplicative group $\mathbf{F}_q - \{0\}$ of $\mathbf{F}_q$
$X(\mathbf{F}_q)$ the set of $\mathbf{F}_q$-rational points of an algebraic variety X
$\#S$ the cardinal of a finite set S

1. Recall: a result of Davenport-Hasse

In this section, we mention classical results due to Stickelberger and due to Davenport and Hasse, recalling the definition of power residue symbols and Jacobi sums.

1.1. Let $\mathbf{F}_q$ denote the finite field of order q. A multiplicative character of $\mathbf{F}_q$ is nothing but a homomorphism of multiplicative groups $\chi : \mathbf{F}_q^\times \to \mathbf{C}^\times$. The trivial character ε is defined by $\varepsilon(\alpha) = 1$ for all $\alpha \in \mathbf{F}_q^\times$. By convention, we set

$$\chi(0) = \begin{cases} 1 & \text{if } \chi \text{ is trivial}, \\ 0 & \text{if } \chi \text{ is non-trivial}. \end{cases}$$

Then we have

$$\sum_{\alpha \in \mathbf{F}_q} \chi(\alpha) = \begin{cases} q & \text{if } \chi \text{ is trivial}, \\ 0 & \text{if } \chi \text{ is non-trivial}. \end{cases}$$

EXAMPLE 1.2. Let n be an integer ≥ 2, and let K be a number field containing all the n-th roots of unity. Take a prime ideal $\mathfrak{p}$ of K not dividing n. For any integer α of K, prime to $\mathfrak{p}$, there exists uniquely an n-th root of unity $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$ such that

$$\alpha^{\frac{N\mathfrak{p}-1}{n}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_n \mod \mathfrak{p}\,,$$

where $N\mathfrak{p}$ denotes the order of the residue field at $\mathfrak{p}$. We call $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$ the n-th power residue symbol. Put $q = N\mathfrak{p}$. Then $\alpha \mapsto \left(\frac{\alpha}{\mathfrak{p}}\right)_n$ induces a multiplicative character of $\mathbf{F}_q$ of order n.

When $n = 2$, $K = \mathbf{Q}$ and p is a prime number $\neq 2$, the power residue symbol is nothing but the Legendre symbol $\left(\frac{\alpha}{p}\right)$.

1.3. Let χ and η be multiplicative characters of the finite field $\mathbf{F}_q$. Then the Jacobi sum $J(\chi, \eta)$ is defined by

$$J(\chi, \eta) = \sum_{\alpha \in \mathbf{F}_q} \chi(\alpha)\eta(1 - \alpha)\,.$$

It is well known that

(1) $J(\chi, \eta) = J(\eta, \chi)$;

(2) $J(\varepsilon, \varepsilon) = q$;

(3) $J(\chi, \varepsilon) = J(\varepsilon, \chi) = 0$ if χ is non-trivial;

(4) $J(\chi, \chi^{-1}) = -\chi(-1)$ if χ is non-trivial;

(5) $|J(\chi, \eta)| = \sqrt{q}$ if χ, η and $\chi\eta$ are non-trivial.

1.4. Now we mention Stickelberger's theorem after a description by Weil [10], which will be used often later. Let n be an integer > 2, and put $\zeta = e^{2\pi i/n}$. Take a prime ideal $\mathfrak{p}$ of the cyclotomic field $\mathbf{Q}(\zeta)$ which is prime to n, and put $q = N\mathfrak{p}$. Let χ denote the multiplicative character of the finite field $\mathbf{F}_q$ induced by $\alpha \mapsto \left(\frac{\alpha}{\mathfrak{p}}\right)_n$. Moreover we define $\sigma_t \in \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ by $\sigma_t(\zeta) = \zeta^t$.

For integers $i, j > 0$, we define

$$w(i, j) = \sum_{\substack{0<t<n \\ (t,n)=1}} \left[\left\langle \frac{ti}{n} \right\rangle + \left\langle \frac{tj}{n} \right\rangle - \left\langle \frac{t(i+j)}{n} \right\rangle\right]\sigma_{-t}^{-1} \in \mathbf{Z}[\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})]\,,$$

where $\langle\lambda\rangle$ denote the fractional part of a real number λ.

Then we have a prime factorization in $\mathbf{Q}(\zeta)$

$$(J(\chi^i, \chi^j)) = \mathfrak{p}^{w(i,j)}$$

for integers $0 < i, j < n$.

1.5. We can now introduce a result due to Davenport and Hasse [4]. Let p be a prime number and q a power of p. Let m and n be positive integers dividing $q - 1$. Let C denote the non-singular projective curve over $\mathbf{F}_q$ defined by the affine equation $ax^m + by^n = c$ ($a, b, c \in \mathbf{F}_q^\times$). Take multiplicative characters χ and η of $\mathbf{F}_q$ of order m and n, respectively. Then we have

$$Z(C/\mathbf{F}_q, t) = \prod_{\substack{0<i<m \\ 0<j<n \\ \chi^i\eta^j\neq\varepsilon}} \left(1 + \chi^i\left(\frac{c}{a}\right)\eta^j\left(\frac{c}{b}\right)J(\chi^i, \eta^j)\,t\right)\Big/(1-t)(1-qt)\,.$$

In particular, we obtain

$$\#C(\mathbf{F}_q) = q + 1 + \sum_{\substack{0<i<m \\ 0<j<n \\ \chi^i\eta^j\neq\varepsilon}} \chi^i\left(\frac{c}{a}\right)\eta^j\left(\frac{c}{b}\right)J(\chi^i, \eta^j)\,.$$

EXAMPLE 1.6. Let p be a prime number ≥ 5, and let E denote the elliptic curve defined by the affine equation $y^2 = x^3 + a$ over the finite field $\mathbf{F}_p$. It is well known that:

(1) Suppose $p \equiv 1 \mod 6$. Then there exists uniquely a pair of integers (A, B) with

$$A^2 + 3B^2 = p\,, \quad A \equiv 1 \mod 3\,, \quad B > 0\,.$$

Put $\pi = A + B\sqrt{-3}$, and let χ and η denote the multiplicative characters of the finite field $\mathbf{F}_p$ induced by $\alpha \mapsto \left(\frac{\alpha}{\pi}\right)_3$ and by $\alpha \mapsto \left(\frac{\alpha}{p}\right)$, respectively. Moreover put $\omega = (-1+\sqrt{-3})/2$. Then we have

$$J(\chi, \eta) = -\pi$$

and therefore, applying the theorem of Davenport-Hasse to the curve E and putting $\varepsilon = \pm 1$, we have:

(a) $\#E(\mathbf{F}_p) = p + 1 - \varepsilon 2A$ if $\chi(a) = 1$ and $\eta(a) = \varepsilon$;

(b) $\#E(\mathbf{F}_p) = p + 1 + \varepsilon(A + 3B)$ if $\chi(a) = \omega$ and $\eta(a) = \varepsilon$;

(c) $\#E(\mathbf{F}_p) = p + 1 + \varepsilon(A - 3B)$ if $\chi(a) = \omega^2$ and $\eta(a) = \varepsilon$.

(2) Suppose $p \equiv 2 \mod 3$. Then we have $\#E(\mathbf{F}_p) = p + 1$.

This result ascends to Gauss' work in Disquisitiones Arithmeticae. For a proof, for example, see [8, 1.6].

REMARK 1.7. Let $P(E; t)$ denote the characteristic polynomial of the Frobenius on E over $\mathbf{F}_p$. The assertion of Example 1.6 is restated as follows:

(1) Suppose $p \equiv 1 \mod 6$. There exists uniquely a pair of integers (A, B) with

$$A^2 + 3B^2 = p\,, \quad A \equiv 1 \mod 3\,, \quad B > 0\,.$$

Put $\pi = A + B\sqrt{-3}$, and let χ and η denote the multiplicative character of $\mathbf{F}_p$ defined by $\alpha \mapsto \left(\frac{\alpha}{\pi}\right)_3$ and $\alpha \mapsto \left(\frac{\alpha}{p}\right)$, respectively. Moreover put $\omega = (-1+\sqrt{-3})/2$ and $\varepsilon = \pm 1$. Then we have:

(a) $P(E; t) = 1 - \varepsilon 2At + pt^2$ if $\chi(a) = 1$ and $\eta(a) = \varepsilon$;

(b) $P(E; t) = 1 + \varepsilon(A + 3B)t + pt^2$ if $\chi(a) = \omega$ and $\eta(a) = \varepsilon$;

(c) $P(E; t) = 1 + \varepsilon(A - 3B)t + pt^2$ if $\chi(a) = \omega^2$ and $\eta(a) = \varepsilon$.

(2) Suppose $p \equiv 5 \mod 6$. Then we have $P(E; t) = 1 + pt^2$.

REMARK 1.8. Let p be a prime number such that $p \equiv 1 \mod 6$, and let E denote the elliptic curve over $\mathbf{F}_p$ defined by the affine equation $y^2 = x^3 + 1$. Then we have

$$\#E(\mathbf{F}_p) \equiv 0 \mod 12$$

as is remarked in [8, Corollary 1.8].

EXAMPLE 1.9. Let p be a prime number ≥ 3, and let $\tilde{E}$ denote the elliptic curve over the finite field $\mathbf{F}_p$ defined by the affine equation $y^2 = x^4 + a$. It is known that:

(1) Suppose $p \equiv 1 \mod 4$. Then there exists uniquely a pair of integers (C, D) with

$$C^2 + D^2 = p\,, \quad C \equiv 1 \mod 4\,, \quad D > 0\,.$$

Put $\rho = C + D\sqrt{-1}$, and let χ denote the multiplicative character of the finite field $\mathbf{F}_p$ induced by $\alpha \mapsto \left(\frac{\alpha}{\rho}\right)_4$. Moreover put $i = \sqrt{-1}$. Then we have

$$\chi(-1)J(\chi, \chi^2) = -\rho\,,$$

and therefore, applying the theorem of Davenport-Hasse to the curve $\tilde{E}$ and putting $\varepsilon = \pm 1$, we have:

(a) $\#\tilde{E}(\mathbf{F}_p) = p + 1 - \varepsilon 2C$ if $\chi(a) = \varepsilon$;

(b) $\#\tilde{E}(\mathbf{F}_p) = p + 1 - \varepsilon 2D$ if $\chi(a) = \varepsilon i$.

(2) Suppose $p \equiv 3 \mod 4$. Then we have $\#\tilde{E}(\mathbf{F}_p) = p + 1$.

We give a proof of the statement for the reader's convenience. Let Q denote the conic over the finite field $\mathbf{F}_p$ defined by the affine equation $y^2 = x^2 + a$. Then a double covering $f : \tilde{E} \to Q$ is defined by $f(x, y) = (x^2, y)$. Moreover we have

$$\#\tilde{E}(\mathbf{F}_p) = \#Q(\mathbf{F}_p) + \sum_{\substack{(\alpha,\beta)\in\mathbf{F}_p^2 \\ \beta^2=\alpha^2+a}} \left(\frac{\alpha}{p}\right).$$

Here $\#Q(\mathbf{F}_p) = p + 1$ since the curve Q is a conic over the finite field $\mathbf{F}_p$.

Suppose $p \equiv 3 \mod 4$. Then we have $\left(\frac{-\alpha}{p}\right) = -\left(\frac{\alpha}{p}\right)$ for each $\alpha \in \mathbf{F}_p^\times$ since $p \equiv 3 \mod 4$. Hence we obtain

$$\sum_{\substack{(\alpha,\beta)\in\mathbf{F}_p^2 \\ \beta^2=\alpha^2+a}} \left(\frac{\alpha}{p}\right) = \sum_{\substack{(\alpha,\beta)\in H\times\mathbf{F}_p \\ \beta^2=\alpha^2+a}} \left\{\left(\frac{\alpha}{p}\right) + \left(\frac{-\alpha}{p}\right)\right\} = 0\,,$$

where $H = \{1, 2, \cdots, \frac{p-1}{2}\}$. Hence we obtain that $\#\tilde{E}(\mathbf{F}_p) = \#Q(\mathbf{F}_p) = p + 1$.

Suppose $p \equiv 1 \mod 4$. Then, applying the theorem of Davenport and Hasse to the curve $\tilde{E}$, we have

$$\#E(\mathbf{F}_p) = p + 1 + \chi(-1)\chi^3(a)J(\chi, \chi^2) + \chi(-1)\chi(a)J(\chi^3, \chi^2)$$

and therefore,

$$\sum_{\substack{(\alpha,\beta)\in\mathbf{F}_p^2 \\ \beta^2=\alpha^2+a}} \left(\frac{\alpha}{p}\right) = \chi(-1)\chi^3(a)J(\chi, \chi^2) + \chi(-1)\chi(a)J(\chi^3, \chi^2)\,.$$

In particular, we have

$$\sum_{\substack{(\alpha,\beta)\in\mathbf{F}_p^2 \\ \beta^2=\alpha^2-1}} \left(\frac{\alpha}{p}\right) = J(\chi, \chi^2) + J(\chi^3, \chi^2)\,.$$

It follows immediately from the definition that the Jacobi sum $J(\chi, \chi^2)$ is a Gauss integer, that is, $J(\chi, \chi^2) \in \mathbf{Z}[\sqrt{-1}]$. Moreover we can verify

$$(J(\chi, \chi^2)) = (\rho)\,,$$

applying Stickelberger's theorem to $n = 4$, $i = 1$, $j = 2$, $\mathfrak{p} = (\rho)$ and noting that

$$w(1,2) = \left[\left\langle\frac{1}{4}\right\rangle + \left\langle\frac{2}{4}\right\rangle - \left\langle\frac{3}{4}\right\rangle\right]\sigma_{-1}^{-1} + \left[\left\langle\frac{3}{4}\right\rangle + \left\langle\frac{6}{4}\right\rangle - \left\langle\frac{9}{4}\right\rangle\right]\sigma_{-3}^{-1} = \sigma_1\,.$$

We have also

$$|J(\chi, \chi^2)| = \sqrt{p}\,, \quad |\rho| = \sqrt{p}$$

as remarked in 1.3. These imply, together with the prime factorization theorem for the ring of Gauss integers, that

$$J(\chi, \chi^2) \in \{\pm\rho, \pm i\rho\}\,.$$

We prove now

$$(\#) \quad \chi(-1)J(\chi, \chi^2) = -p\,.$$

At first put

$$R = \left\{(\alpha, \beta) \in \mathbf{F}_p^2\,;\ \beta^2 = \alpha^2 - 1,\ \left(\frac{\alpha}{p}\right) = 1\right\},$$

$$S = \left\{(\alpha, \beta) \in \mathbf{F}_p^2\,;\ \beta^2 = \alpha^2 - 1,\ \left(\frac{\alpha}{p}\right) = -1\right\},$$

$$T = \left\{(\alpha, \beta) \in \mathbf{F}_p^2\,;\ \beta^2 = \alpha^2 - 1,\ \left(\frac{\alpha}{p}\right) = 0\right\}$$

and

$$r = \#R\,, \quad s = \#S\,, \quad t = \#T\,.$$

Then we have

$$Q(\mathbf{F}_p) - \{\infty_+, \infty_-\} = R \cup S \cup T$$

and

$$p - 1 = r + s + t\,,$$

where Q is the conic over $\mathbf{F}_p$ defined by the affine equation $y^2 = x^2 - 1$. This implies that

$$\sum_{\substack{(\alpha,\beta)\in\mathbf{F}_p^2 \\ \beta^2=\alpha^2-1}} \left(\frac{\alpha}{p}\right) = r - s = 2r + t - p + 1\,.$$

Furthermore we have a partition

$$R = \left\{(\alpha, \beta) \in (\mathbf{F}_p^\times)^2 \ ; \ \beta^2 = \alpha^2 - 1, \ \left(\frac{\alpha}{p}\right) = 1\right\} \cup \{(\pm 1, 0)\}\,,$$

and the group $\boldsymbol{\mu}_2 \times \boldsymbol{\mu}_2$ acts faithfully on $R - \{(\pm 1, 0)\}$ by $(\xi, \theta)(\alpha, \beta) = (\xi\alpha, \theta\beta)$ since $\left(\frac{-\alpha}{p}\right) = \left(\frac{\alpha}{p}\right)$ for each $\alpha \in \mathbf{F}_p$. It follows that $r \equiv 2 \mod 4$. On the other hand, we have $t = 2$, that is, there exist exactly two elements $\beta \in \mathbf{F}_p^\times$ such that $\beta^2 = -1$ since $p \equiv 1 \mod 4$. Summing up, we have gotten

$$\sum_{\substack{(\alpha,\beta)\in\mathbf{F}_p^2 \\ \beta^2=\alpha^2-1}} \left(\frac{\alpha}{p}\right) = 3 - p + 2r \equiv \begin{cases} -2 \mod 8 & \text{if } p \equiv 1 \mod 8\,, \\ 2 \mod 8 & \text{if } p \equiv 5 \mod 8\,, \end{cases}$$

which implies

$$\mathrm{Tr} J(\chi, \chi^2) \equiv \begin{cases} -2 \mod 8 & \text{if } p \equiv 1 \mod 8\,, \\ 2 \mod 8 & \text{if } p \equiv 5 \mod 8\,. \end{cases}$$

Here Tr denote the trace for the quadratic extension $\mathbf{Q}(\sqrt{-1})/\mathbf{Q}$.

Note now that

$$\mathrm{Tr}(\rho) = 2C\,, \quad \mathrm{Tr}(i\rho) = -2D\,,$$

which implies

$$\mathrm{Tr}(\rho) \equiv 2 \mod 8\,, \quad \mathrm{Tr}(\pm i\rho) \equiv 0 \mod 4$$

and

$$\mathrm{Tr}(-\rho) \equiv -2 \mod 8$$

since $C \equiv 1 \mod 4$, $D \equiv 0 \mod 2$.

Hence we obtain

$$J(\chi, \chi^2) = \begin{cases} -\rho & \text{if } p \equiv 1 \mod 8\,, \\ \rho & \text{if } p \equiv 5 \mod 8\,. \end{cases}$$

It follows that $\chi(-1)J(\chi, \chi^2) = -\rho$, and therefore we have

(a) $\#\tilde{E}(\mathbf{F}_p) = p + 1 + \mathrm{Tr}(-\varepsilon\rho) = p + 1 - \varepsilon 2C$ if $\chi(a) = \varepsilon$;

(b) $\#\tilde{E}(\mathbf{F}_p) = p + 1 + \mathrm{Tr}(\varepsilon i\rho) = p + 1 - \varepsilon 2D$ if $\chi(a) = \varepsilon i$.

REMARK 1.10. Let $P(\tilde{E}; t)$ denote the characteristic polynomial of the Frobenius on $\tilde{E}$ over $\mathbf{F}_p$. The assertion of Example 1.9 is restated as follows:

(1) Suppose $p \equiv 1 \mod 4$. There exists uniquely a pair of integers (C, D) with

$$C^2 + D^2 = p\,, \quad C \equiv 1 \mod 4\,, \quad D > 0\,.$$

Put $\rho = C+D\sqrt{-1}$, and let χ denote the multiplicative character of $\mathbf{F}_p$ defined by $\alpha \mapsto \left(\frac{\alpha}{\rho}\right)_4$. Moreover put $i = \sqrt{-1}$. Then we have:

(a) $P(\tilde{E};t) = 1 - \varepsilon 2Ct + pt^2$ if $\chi(a) = \varepsilon$;

(c) $P(\tilde{E};t) = 1 - \varepsilon 2Dt + pt^2$ if $\chi(a) = \varepsilon i$.

(2) Suppose $p \equiv 3 \mod 4$. Then we have $P(\tilde{E};t) = 1 + pt^2$.

2. Congruence zeta function of the curve $y^2 = x^6 + a$

Throughout the section, we put $\zeta = e^{\pi i/3}$.

PROPOSITION 2.1. *Let p be a prime number ≥ 5, and let X denote the hyperelliptic curve over the finite field $\mathbf{F}_p$ defined by the affine equation $y^2 = x^6 + a$.*

(1) *Suppose $p \equiv 1 \mod 6$. Then there exists uniquely a pair of integers (A, B) with*

$$A^2 + 3B^2 = p\,, \quad A \equiv 1 \mod 3\,, \quad B > 0\,.$$

Put $\pi = A + B\sqrt{-3}$ and let χ denote the multiplicative characters of the finite field $\mathbf{F}_p$ induced by $\alpha \mapsto \left(\frac{\alpha}{\pi}\right)_3$. Put $\omega = (-1+\sqrt{-3})/2$. Moreover let E denote the elliptic curve over the finite field $\mathbf{F}_p$ defined by the affine equation $y^2 = x^3 + a$. Then we have:

(a) $\#X(\mathbf{F}_p) - \#E(\mathbf{F}_p) = -2A$ *if* $\chi(a) = 1$;

(b) $\#X(\mathbf{F}_p) - \#E(\mathbf{F}_p) = A - 3B$ *if* $\chi(a) = \omega$;

(c) $\#X(\mathbf{F}_p) - \#E(\mathbf{F}_p) = A + 3B$ *if* $\chi(a) = \omega^2$.

(2) *Suppose $p \equiv 5 \mod 6$. Then we have $\#X(\mathbf{F}_p) = p + 1$.*

PROOF. Suppose $p \equiv 5 \mod 6$. Let Q denote the conic over the finite field $\mathbf{F}_p$ defined by the affine equation $y^2 = x^2 + a$. Then a triple covering $f : X \to Q$ is defined by $f(x, y) = (x^3, y)$. The curves X and Q have two infinity points, and $\alpha \mapsto \alpha^3$ is bijective on $\mathbf{F}_p$ since $p \equiv 2 \mod 3$. Hence we obtain $\#X(\mathbf{F}_p) = \#Q(\mathbf{F}_p) = p + 1$.

Suppose $p \equiv 1 \mod 6$. Let $\tilde{\chi}$ denote the multiplicative character of the finite field $\mathbf{F}_p$ induced by $\alpha \mapsto \left(\frac{\alpha}{\pi}\right)_6$. Then, applying the theorem of Davenport-Hasse to the curves X and E, we have

$$\#X(\mathbf{F}_p) - \#E(\mathbf{F}_p) = \mathrm{Tr}_{\mathbf{Q}(e^{\pi i/3})/\mathbf{Q}}(\tilde{\chi}(-1)\tilde{\chi}^4(a)J(\tilde{\chi}, \tilde{\chi}^3))\,.$$

Hence the result is a direct consequence of the following Theorem 2.2.

THEOREM 2.2 *Let p be a prime number with $p \equiv 1 \mod 6$. Then there exists uniquely a pair of integers (A, B) with*

$$A^2 + 3B^2 = p\,, \quad A \equiv 1 \mod 3\,, \quad B > 0\,.$$

Put $\pi = A + B\sqrt{-3}$ and let $\tilde{\chi}$ denote the multiplicative character of the finite field $\mathbf{F}_p$ induced by $\alpha \mapsto \left(\frac{\alpha}{\pi}\right)_6$. Then we have

$$\tilde{\chi}(-1)J(\tilde{\chi}, \tilde{\chi}^3) = -\pi\,.$$

2.3. We start to prove Theorem 2.2 by the following observation. Let E denote the curve over the finite field $\mathbf{F}_p$ defined by the affine equation $y^2 = x^3 + a$. Then a double covering $f : X \to E$ is defined by $f(x, y) = (x^2, y)$. Moreover we have

$$\#X(\mathbf{F}_p) = \#E(\mathbf{F}_p) + 1 + \sum_{\substack{(\alpha,\beta)\in\mathbf{F}_p^2 \\ \beta^2=\alpha^3+a}} \left(\frac{\alpha}{p}\right)$$

since X has two infinity points while E has one infinity point.

We present Lemma 2.4 and Corollary 2.5, which are available to prove Theorem 2.2.

LEMMA 2.4. *Let p be a prime number such that $p \equiv 1 \mod 6$. Then there exists uniquely a pair of integers (A, B) such that $A^2 + 3B^2 = p$, $A \equiv 1 \mod 3$ and $B > 0$. Put $\pi = A + B\sqrt{-3}$. Let $\tilde{\chi}$ denote the multiplicative character of the finite field $\mathbf{F}_p$ induced by $\alpha \mapsto \left(\frac{\alpha}{\pi}\right)_6$. Then we have*:

$$\mathrm{Tr}(\tilde{\chi}(-1)\tilde{\chi}^4(a)J(\tilde{\chi}, \tilde{\chi}^3)) = 1 + \sum_{\substack{(\alpha,\beta)\in\mathbf{F}_p^2 \\ \beta^2=\alpha^3+a}} \left(\frac{\alpha}{p}\right),$$

where Tr *denotes the trace for the extension $\mathbf{Q}(\zeta)/\mathbf{Q}$.*

PROOF. Let X denote the hyperelliptic curve over $\mathbf{F}_p$ defined by the affine equation $y^2 = x^6 + a$ and let E denote the elliptic curve over $\mathbf{F}_p$ defined by the affine equation $y^2 = x^3 + a$. Applying the theorem of Davenport-Hasse to the curves X and E, we obtain

$$\begin{aligned}\#X(\mathbf{F}_p) = p + 1 &+ \tilde{\chi}^5(a)J(\tilde{\chi}^2, \tilde{\chi}^3) + \tilde{\chi}(a)J(\tilde{\chi}^4, \tilde{\chi}^3) \\ &+ \tilde{\chi}(-1)\tilde{\chi}^4(a)J(\tilde{\chi}, \tilde{\chi}^3) + \tilde{\chi}(-1)\tilde{\chi}^2(a)J(\tilde{\chi}^5, \tilde{\chi}^3)\end{aligned}$$

and

$$\#E(\mathbf{F}_p) = p + 1 + \tilde{\chi}^5(a)J(\tilde{\chi}^2, \tilde{\chi}^3) + \tilde{\chi}(a)J(\tilde{\chi}^4, \tilde{\chi}^3).$$

It follows that

$$\#X(\mathbf{F}_p) = \#E(\mathbf{F}_p) + \mathrm{Tr}(\tilde{\chi}(-1)\tilde{\chi}^4(a)J(\tilde{\chi}, \tilde{\chi}^3))$$

since the orbit of $\tilde{\chi}(-1)\tilde{\chi}^4(a)J(\tilde{\chi}, \tilde{\chi}^3)$ under the action by $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ is given by

$$\{\tilde{\chi}(-1)\tilde{\chi}^4(a)J(\tilde{\chi}, \tilde{\chi}^3), \tilde{\chi}(-1)\tilde{\chi}^2(a)J(\tilde{\chi}^5, \tilde{\chi}^3)\}.$$

On the other hand, we have

$$\#X(\mathbf{F}_p) = \#E(\mathbf{F}_p) + 1 + \sum_{\substack{(\alpha,\beta)\in\mathbf{F}_p^2 \\ \beta^2=\alpha^3+a}} \left(\frac{\alpha}{p}\right).$$

COROLLARY 2.5. *Under the notations of* 2.4, *we have*

$$\mathrm{Tr}\,(\tilde{\chi}(-1)J(\tilde{\chi},\tilde{\chi}^3)) \equiv -2 \mod 6\,.$$

PROOF. Put

$$R = \left\{(\alpha,\beta)\in \mathbf{F}_p^2\,;\ \beta^2=\alpha^3+1,\ \left(\frac{\alpha}{p}\right)=1\right\},$$

$$S = \left\{(\alpha,\beta)\in \mathbf{F}_p^2\,;\ \beta^2=\alpha^3+1,\ \left(\frac{\alpha}{p}\right)=-1\right\},$$

$$T = \left\{(\alpha,\beta)\in \mathbf{F}_p^2\,;\ \beta^2=\alpha^3+1,\ \left(\frac{\alpha}{p}\right)=0\right\}$$

and

$$r=\#R\,,\quad s=\#S\,,\quad t=\#T\,.$$

Then we have

$$E(\mathbf{F}_p)-\{\infty\}=R\cup S\cup T$$

and

$$\#E(\mathbf{F}_p)-1=r+s+t\,,$$

where E is the elliptic curve over $\mathbf{F}_p$ defined by the affine equation $y^2=x^3+1$. This implies that

$$1+\sum_{\substack{(\alpha,\beta)\in\mathbf{F}_p^2\\ \beta^2=\alpha^3+1}}\left(\frac{\alpha}{p}\right)=1+r-s=2r+t-\#E(\mathbf{F}_p)+2\,.$$

Hence we obtain the result from (a) $r \equiv \begin{cases} 3 \mod 6 & \text{if } p\equiv 1 \mod 12, \\ 0 \mod 6 & \text{if } p\equiv 7 \mod 12 \end{cases}$; (b) $t=2$; (c) $\#E(\mathbf{F}_p)\equiv 0 \mod 12$.

In order to verify (a), we consider an action of $\boldsymbol{\mu}_3\times\boldsymbol{\mu}_2$. If $p\equiv 1 \mod 12$, then we have $\left(\frac{\zeta}{p}\right)=1$. Hence we obtain

$$R = \left\{(\alpha,\beta)\in (\mathbf{F}_p^\times)^2\,;\ \beta^2=\alpha^3+1,\ \left(\frac{\alpha}{p}\right)=1\right\}\cup\{(-1,0),(\zeta,0),(\zeta^5,0)\}\,.$$

Moreover the group $\boldsymbol{\mu}_3\times\boldsymbol{\mu}_2$ acts faithfully on $R-\{(-1,0),(\zeta,0),(\zeta^5,0)\}$ by $(\xi,\theta)(\xi,\beta)=(\xi\alpha,\theta\beta)$ since $\left(\frac{\zeta^2\alpha}{p}\right)=\left(\frac{\alpha}{p}\right)$ for each $\alpha\in\mathbf{F}_p$. Hence (a) follows. If $p\equiv 7 \mod 12$, then we have $\left(\frac{\zeta}{p}\right)=-1$. This implies that

$$R = \left\{(\alpha,\beta)\in (\mathbf{F}_p^\times)^2\,;\ \beta^2=\alpha^3+1,\ \left(\frac{\alpha}{p}\right)=1\right\}.$$

Therefore we obtain (a) as above.

It is easy to verify (b). In fact, there exist exactly two elements $1, -1 \in \mathbf{F}_p^\times$ such that $\beta^2 = 1$. The assertion (c) follows from Remark 1.8.

2.6. Proof of Theorem 2.2. We have a prime factorization

$$(p) = (\pi)(\bar{\pi})$$

in $\mathbf{Q}(\zeta)$. Let $\tilde{\chi}$ denote the multiplicative character of the finite field $\mathbf{F}_p$ induced by $\alpha \mapsto \left(\frac{\alpha}{\pi}\right)_6$.

It follows immediately from the definition that the Jacobi sum $J(\tilde{\chi}, \tilde{\chi}^3)$ is an Eisenstein integer, that is, $J(\tilde{\chi}, \tilde{\chi}^3) \in \mathbf{Z}[\zeta]$. Moreover we can verify

$$(J(\tilde{\chi}, \tilde{\chi}^3)) = (\pi)\,,$$

applying Stickelberger's theorem to $n = 6$, $i = 1$, $j = 3$, $\mathfrak{p} = (\pi)$ and noting that

$$w(1,3) = \left[\left\langle\frac{1}{6}\right\rangle + \left\langle\frac{3}{6}\right\rangle - \left\langle\frac{4}{6}\right\rangle\right]\sigma_{-1}^{-1} + \left[\left\langle\frac{5}{6}\right\rangle + \left\langle\frac{15}{6}\right\rangle - \left\langle\frac{20}{6}\right\rangle\right]\sigma_{-5}^{-1} = \sigma_1\,.$$

We have also

$$|J(\tilde{\chi}, \tilde{\chi}^3)| = \sqrt{p},\ |\pi| = \sqrt{p}$$

as is remarked in 1.3. These imply, together with the prime factorization theorem for the ring of Eisenstein integers, that

$$J(\tilde{\chi}, \tilde{\chi}^3) \in \{\pm\pi, \pm\zeta\pi, \pm\zeta^2\pi\}\,.$$

By Corollary 2.5, we have

$$\mathrm{Tr}\,(\tilde{\chi}(-1)J(\tilde{\chi}, \tilde{\chi}^3)) \equiv -2 \mod 6\,.$$

On the other hand, we have

$$\mathrm{Tr}(\pi) = 2A\,, \quad \mathrm{Tr}(\zeta\pi) = A - 3B\,, \quad \mathrm{Tr}(\zeta^2\pi) = -A - 3B\,,$$

which implies

$$\mathrm{Tr}(\pi) = 2 \mod 6\,, \quad \mathrm{Tr}(\zeta\pi) = \mathrm{Tr}(-\zeta^2\pi) \equiv 1 \mod 6$$

and

$$\mathrm{Tr}(-\pi) = -2 \mod 6\,, \quad \mathrm{Tr}(-\zeta\pi) = \mathrm{Tr}(\zeta^2\pi) \equiv -1 \mod 6\,.$$

since $A \equiv 1 \mod 3$ and $B \equiv 0 \mod 2$.

Hence we obtain

$$\tilde{\chi}(-1)J(\tilde{\chi}, \tilde{\chi}^3) = -\pi\,.$$

2.7. Let p be a prime number which is prime to 6. Let X denote the hyperelliptic curve over $\mathbf{F}_p$ defined by the affine equation $y^2 = x^6 + a$ over $\mathbf{F}_p$, and let E denote the elliptic curve defined by the affine equation $y^2 = x^3 + a$. Let $J(X)$ denote the Jacobian variety of X. Then the double covering $X \to E$ defined by $(x, y) \mapsto (x^2, y)$ induces a homomorphism of abelian varieties $E \to J(X)$. Put $S = \mathrm{Coker}[E \to J(X)]$. Then S is an elliptic curve over $\mathbf{F}_p$, and $J(X)$ is isogenous to the product $E \times S$.

Let $P(J(X)/\mathbf{F}_p; t)$, $P(E/\mathbf{F}_p; t)$ and $P(S/\mathbf{F}_p; t)$ denote the characteristic polynomials of the Frobenius on $J(X)$, E and S over $\mathbf{F}_p$, respectively. Then we have

$$(1-t)(1-pt)Z(X/\mathbf{F}_p; t) = P(J(X)/\mathbf{F}_p; t)$$

and

$$P(J(X)/\mathbf{F}_p; t) = P(E/\mathbf{F}_p; t)P(S/\mathbf{F}_p; t)\,.$$

COROLLARY 2.8. *Under the notation of* 2.7, *we put* $P(t) = P(S/\mathbf{F}_p; t)$. *Then*:

(1) *Suppose* $p \equiv 1 \mod 6$. *There exists uniquely a pair of integers* (A, B) *with*

$$A^2 + 3B^2 = p\,, \quad A \equiv 1 \mod 3\,, \quad B > 0\,.$$

Put $\pi = A + B\sqrt{-3}$, *and let* χ *denote the multiplicative character of* $\mathbf{F}_p$ *defined by* $\alpha \mapsto \left(\frac{\alpha}{\pi}\right)_3$. *Moreover put* $\omega = (-1 + \sqrt{-3})/2$. *Then we have*:

(a) $P(t) = 1 - 2At + pt^2$ *if* $\chi(a) = 1$;

(b) $P(t) = 1 + (A - 3B)t + pt^2$ *if* $\chi(a) = \omega$;

(c) $P(t) = 1 + (A + 3B)t + pt^2$ *if* $\chi(a) = \omega^2$.

(2) *Suppose* $p \equiv 5 \mod 6$. *Then we have* $P(t) = 1 + pt^2$.

PROOF. Proof of (1). Let $\tilde{\chi}$ denote the multiplicative characters of the finite field $\mathbf{F}_p$ induced by $\alpha \mapsto \left(\frac{\alpha}{\pi}\right)_6$. Then, by the theorem of Davenport-Hasse and 2.7, we have

$$P(t) = (1 + \tilde{\chi}(-1)\tilde{\chi}^4(a)J(\tilde{\chi}, \tilde{\chi}^3)\,t)(1 + \tilde{\chi}(-1)\tilde{\chi}^2(a)J(\tilde{\chi}^5, \tilde{\chi}^3)\,t)\,.$$

Furthermore we have

$$\tilde{\chi}(-1)J(\tilde{\chi}, \tilde{\chi}^3) = -(A + B\sqrt{-3})$$

and therefore

$$\tilde{\chi}(-1)J(\tilde{\chi}^5, \tilde{\chi}^3) = -(A - B\sqrt{-3})$$

as is proved in Theorem 2.2. Hence we obtain the result, expanding the right hand side in each case.

Proof of (2). Let α_1, α_2 denote the eigenvalues of the Frobenius on the elliptic curve $S = \mathrm{Coker}[E \to J(X)]$ over $\mathbf{F}_p$. Then we have

$$\alpha_1 + \alpha_2 = 0$$

since $\#X(\mathbf{F}_p) = p + 1$ as is shown in Proposition 2.1. It follows that

$$\alpha_1, \alpha_2 \in \{\sqrt{-p}, -\sqrt{-p}\}\,.$$

Hence we obtain

$$P(t) = 1 + pt^2 .$$

COROLLARY 2.9. *Let p be a prime number such that $p \equiv 1 \mod 12$, and let X denote the hyperelliptic curve over $\mathbf{F}_p$ defined by the affine equation $y^2 = x^6 - 1$. Then we have*:

(1) $\#X(\mathbf{F}_p) \equiv -2 \mod 24$ *if* $p \equiv 1 \mod 24$;

(2) $\#X(\mathbf{F}_p) \equiv 10 \mod 24$ *if* $p \equiv 13 \mod 24$.

PROOF. Take $A, B \in \mathbf{Z}$ such that $A^2 + 3B^2 = p$ and $A \equiv 1 \mod 3$. Then we have $\#X(\mathbf{F}_p) = p + 1 - 4A$ since $\chi(-1) = 1$, as is shown in Proposition 2.1 and Example 1.6. Now, assume that $A \equiv 4 \mod 6$, then we would have $B^2 \equiv -1 \mod 4$. Therefore, we obtain $A \equiv 1 \mod 6$.

COROLLARY 2.10. *Let p be a prime number which is prime to 6, and let X denote the hyperelliptic curve over $\mathbf{F}_p$ defined by the affine equation $y^2 = x^6 - 1$. Then we have*:

$$\#X(\mathbf{F}_{p^2}) \equiv -2 \mod 24 .$$

PROOF. In the case $p \equiv 7 \mod 12$, take $A, B \in \mathbf{Z}$ such that $A^2 + 3B^2 = p$ and $A \equiv 1 \mod 3$, $B > 0$. Then we have $\#X(\mathbf{F}_{p^2}) = p^2 + 1 - 2\{(A + B\sqrt{-3})^2 + (A - B\sqrt{-3})^2\} = p^2 + 1 - 8A^2 + 4p$ since $\chi(-1) = -1$, as is shown in Corollary 2.8 and Remark 1.7.

In the case $p \equiv 5$ or $11 \mod 12$, we have $\#X(\mathbf{F}_{p^2}) = p^2 + 1 + 4p = (p + 1)^2 + 2p$ as is shown in Corollary 2.8 and Remark 1.7.

REMARK 2.11. Let p be a prime number which is prime to 6. Let X denote the hyperelliptic curve over $\mathbf{F}_p$ defined by the affine equation $y^2 = x^6 + a$ over $\mathbf{F}_p$, and let E denote the elliptic curve defined by the affine equation $y^2 = x^3 + a$. Put $S = \mathrm{Coker}[E \to J(X)]$.

By Tate's conjecture for Abelian varieties over a finite fields, we can conclude that:

(a) If $p \equiv 1 \mod 6$, S is isogenous to the ordinary elliptic curve over the finite field $\mathbf{F}_p$ defined by $y^2 = x^3 + a^2$;

(b) If $p \equiv 5 \mod 6$, S is isogenous to the supersingular elliptic curve over the finite field $\mathbf{F}_p$ defined by $y^2 = x^3 + 1$,
comparing the congruence zeta functions of E and S (Remark 1.7 and Corollary 2.8).

3. Counting points of the curve $y^2 = x^{12} + a$

Throughout the section, we put $\zeta = e^{\pi i/6}$.

PROPOSITION 3.1. *Let Y denote the hyperelliptic curve over the finite field $\mathbf{F}_p$ defined by the affine equation $y^2 = x^{12} + a$.*

(1) *Suppose* $p \equiv 1 \mod 12$. *There exist unique pairs of integers* (A, B) *and* (C, D) *with*

$$A^2 + 3B^2 = p\,, \quad A \equiv 1 \mod 3\,, \quad B > 0$$

and

$$C^2 + D^2 = p\,, \quad C \equiv 1 \mod 4\,, \quad D > 0\,.$$

Put $\pi = A + B\sqrt{-3}$ *and* $\rho = C + D\sqrt{-1}$, *and let* χ *denote the multiplicative character of* $\mathbf{F}_p$ *defined by* $\alpha \mapsto \left(\frac{\alpha}{\pi, \rho}\right)_{12}$. *Moreover let* X *denote the hyperelliptic curve over the finite field* $\mathbf{F}_p$ *defined by the affine equation* $y^2 = x^6 + a$ *and put* $\varepsilon = \pm 1$.

If $C \not\equiv 0 \mod 3$, *then we have*:
(a) $\#Y(\mathbf{F}_p) - \#X(\mathbf{F}_p) = -\varepsilon 6C$ *if* $\chi(a) = \varepsilon$;
(b) $\#Y(\mathbf{F}_p) - \#X(\mathbf{F}_p) = -\varepsilon 2D$ *if* $\chi(a) = \varepsilon\zeta^3$;
(c) $\#Y(\mathbf{F}_p) - \#X(\mathbf{F}_p) = -\varepsilon 4D$ *if* $\chi(a) = \varepsilon\zeta$ *or* $\varepsilon\zeta^5$;
(d) $\#Y(\mathbf{F}_p) = \#X(\mathbf{F}_p)$ *if* $\chi(a) = \varepsilon\zeta^4$ *or* $\varepsilon\zeta^2$.

If $C \equiv 0 \mod 3$, *then we have*:
(a) $\#Y(\mathbf{F}_p) - \#X(\mathbf{F}_p) = \varepsilon 2C$ *if* $\chi(a) = \varepsilon$;
(b) $\#Y(\mathbf{F}_p) - \#X(\mathbf{F}_p) = \varepsilon 6D$ *if* $\chi(a) = \varepsilon\zeta^3$;
(c) $\#Y(\mathbf{F}_p) = \#X(\mathbf{F}_p)$ *if* $\chi(a) = \varepsilon\zeta$ *or* $\varepsilon\zeta^5$;
(d) $\#Y(\mathbf{F}_p) - \#X(\mathbf{F}_p) = -\varepsilon 4C$ *if* $\chi(a) = \varepsilon\zeta^4$ *or* $-\varepsilon\zeta^2$.

(2) *Suppose* $p \equiv 5 \mod 12$. *Let* $\tilde{E}$ *denote the elliptic curve over the finite field* $\mathbf{F}_p$ *defined by the affine equation* $y^2 = x^4 + a$. *Then we have*

$$\#Y(\mathbf{F}_p) = \#\tilde{E}(\mathbf{F}_p)\,.$$

(3) *Suppose* $p \equiv 7 \mod 12$. *Let* X *denote the hyperelliptic curve over the finite field* $\mathbf{F}_p$ *defined by the affine equation* $y^2 = x^6 + a$. *Then we have*

$$\#Y(\mathbf{F}_p) = \#X(\mathbf{F}_p)\,.$$

(4) *Suppose* $p \equiv 11 \mod 12$. *Then we have* $\#Y(\mathbf{F}_p) = p + 1$.

3.2. Proof of (2) and (4). Let $\tilde{E}$ denote the elliptic curve over the finite field $\mathbf{F}_p$ defined by the affine equation $y^2 = x^4 + a$. Then a triple covering $f : Y \to \tilde{E}$ is defined by $f(x, y) = (x^3, y)$. The curves X and $\tilde{E}$ have two infinity points, and the map $\alpha \to \alpha^3$ is bijective on $\mathbf{F}_p$ since $p \equiv 2 \mod 3$. Hence we obtain $\#Y(\mathbf{F}_p) = \#\tilde{E}(\mathbf{F}_p)$.

3.3. Proof of (3). Let X denote the hyperelliptic curve over the finite field $\mathbf{F}_p$ defined by the affine equation $y^2 = x^6 + a$. Then a double covering $f : Y \to X$ is defined by $f(x, y) = (x^2, y)$. Moreover put

$$R = \left\{(\alpha, \beta) \in \mathbf{F}_p^2\,;\ \beta^2 = \alpha^6 + a,\ \left(\frac{\alpha}{p}\right) = 1\right\},$$

$$S = \left\{ (\alpha, \beta) \in \mathbf{F}_p^2 \,;\; \beta^2 = \alpha^6 + a,\ \left(\frac{\alpha}{p}\right) = -1 \right\}$$

and

$$r = \#R\,, \quad s = \#S\,,$$

then we have

$$\#Y(\mathbf{F}_p) = \#X(\mathbf{F}_p) + \sum_{\substack{(\alpha,\beta)\in\mathbf{F}_p^2 \\ \beta^2=\alpha^6+a}} \left(\frac{\alpha}{p}\right) = \#X(\mathbf{F}_p) + r - s\,.$$

Now, denote by ζ_6 a primitive 6th root of unity in $\mathbf{F}_p$, then we have $\left(\frac{\zeta\alpha}{p}\right) = -\left(\frac{\alpha}{p}\right)$ for each $\alpha \in \mathbf{F}_p^\times$ since $p \equiv 7 \mod 12$. Hence, a bijective map $R \to S$ is defined by $\alpha \mapsto \xi_6\alpha$. This implies that $r = s$. Hence we obtain that $\#Y(\mathbf{F}_p) = \#X(\mathbf{F}_p)$.

3.4. Proof of (1). Applying the theorem of Davenport-Hasse to the curves Y and X, we have

$$\begin{aligned}\#Y(\mathbf{F}_p) - \#X(\mathbf{F}_p) &= \mathrm{Tr}_{\mathbf{Q}(e^{\pi i/6})/\mathbf{Q}}(\chi(-1)\chi^7(a)J(\chi, \chi^6)) \\ &\quad + \mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}(\chi(-1)\chi^9(a)J(\chi^3, \chi^6))\,.\end{aligned}$$

Hence the result is a direct consequence of the following Theorem 3.5 and Example 1.9.

THEOREM 3.5. *Let p be a prime number with $p \equiv 1 \mod 12$. Then there exist unique pairs of integers (A, B) and (C, D) with*

$$A^2 + 3B^2 = p\,, \quad A \equiv 1 \mod 3\,, \quad B > 0$$

and

$$C^2 + D^2 = p\,, \quad C \equiv 1 \mod 4\,, \quad D > 0\,.$$

Put $\pi = A + B\sqrt{-3}$ and $\rho = C + D\sqrt{-1}$, and let χ denote the multiplicative character of $\mathbf{F}_p$ defined by $\alpha \mapsto \left(\frac{\alpha}{\pi,\rho}\right)_{12}$. Then we have

$$\chi(-1)J(\chi, \chi^6) = \begin{cases} -\rho & \text{if } C \not\equiv 0 \mod 3\,, \\ \rho & \text{if } C \equiv 0 \mod 3\,. \end{cases}$$

We present Lemma 3.6 and Corollary 3.7, which are available to verify Theorem 3.5 and to prove the theorem stated in the next section.

LEMMA 3.6. *Let $\mathfrak{p}$ be a prime ideal of $\mathbf{Q}(\zeta)$. Assume that $\mathfrak{p}$ is prime to 6, and put $q = N\mathfrak{p}$. Let χ denote the multiplicative character of $\mathbf{F}_q$ defined by $\alpha \mapsto \left(\frac{\alpha}{\mathfrak{p}}\right)_{12}$. Then we* *have*:

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\chi(-1)\chi^7(a)J(\chi,\chi^6)) + \mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}\big(\chi(-1)\chi^9(a)J(\chi^3,\chi^6)\big) = \sum_{\substack{(\alpha,\beta)\in\mathbf{F}_q^2\\ \beta^2=\alpha^6+a}} \left(\frac{\alpha}{\mathfrak{p}}\right)_2 .$$

PROOF. Let Y and X denote the hyperelliptic curves over the finite field $\mathbf{F}_q$ defined by the affine equation $y^2 = x^{12} + a$ and by the affine equation $y^2 = x^6 + a$, respectively. Applying the theorem of Davenport-Hasse to the curves Y and X, we obtain

$$\begin{aligned}\#Y(\mathbf{F}_q) = q + 1 &+ \chi^8(a)J(\chi^2,\chi^6) + \chi^{10}(a)J(\chi^4,\chi^6) + \chi^2(a)J(\chi^8,\chi^6)\\ &+ \chi^4(a)J(\chi^{10},\chi^6) + \chi(-1)\chi^7(a)J(\chi,\chi^6) + \chi(-1)\chi^{11}(a)J(\chi^5,\chi^6)\\ &+ \chi(-1)\chi(a)J(\chi^7,\chi^6) + \chi(-1)\chi^5(a)J(\chi^{11},\chi^6)\\ &+ \chi(-1)\chi^9(a)J(\chi^3,\chi^6) + \chi(-1)\chi^3(a)J(\chi^9,\chi^6)\end{aligned}$$

and

$$\begin{aligned}\#X(\mathbf{F}_q) = q + 1 &+ \chi^8(a)J(\chi^2,\chi^6) + \chi^{10}(a)J(\chi^4,\chi^6)\\ &+ \chi^2(a)J(\chi^8,\chi^6) + \chi^4(a)J(\chi^{10},\chi^6) .\end{aligned}$$

It follows that

$$\begin{aligned}\#Y(\mathbf{F}_q) = \#X(\mathbf{F}_q) &+ \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\chi(-1)\chi^7(a)J(\chi,\chi^6))\\ &+ \mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}(\chi(-1)\chi^9(a)J(\chi^3,\chi^6))\end{aligned}$$

since the orbit of $\chi(-1)\chi^7(a)J(\chi,\chi^6)$ under the action by Gal$(\mathbf{Q}(\zeta)/\mathbf{Q})$ is given by

$$\begin{gathered}\{\chi(-1)\chi^7(a)J(\chi,\chi^6), \chi(-1)\chi^{11}(a)J(\chi^5,\chi^6),\\ \chi(-1)\chi(a)J(\chi^7,\chi^6), \chi(-1)\chi^5(a)J(\chi^{11},\chi^6)\}\end{gathered}$$

and the orbit of $\chi(-1)\chi^9(a)J(\chi^3,\chi^6)$ under the action by Gal$(\mathbf{Q}(\sqrt{-1})/\mathbf{Q})$ is given by

$$\{\chi(-1)\chi^9(a)J(\chi^3,\chi^6),\ \chi(-1)\chi^3(a)J(\chi^9,\chi^6)\} .$$

On the other hand, we have

$$\#Y(\mathbf{F}_q) = \#X(\mathbf{F}_q) + \sum_{\substack{(\alpha,\beta)\in\mathbf{F}_q^2\\ \beta^2=\alpha^6+a}} \left(\frac{\alpha}{\mathfrak{p}}\right)_2 .$$

Hence the required result.

COROLLARY 3.7. *Under the notations of* 3.6, *we have*

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(J(\chi,\chi^6)) + \mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}\big(J(\chi^3,\chi^6)\big) \equiv \begin{cases} -6 \mod 24 & \text{if } q \equiv 1 \mod 24 ,\\ 6 \mod 24 & \text{if } q \equiv 13 \mod 24 .\end{cases}$$

PROOF. Put

$$R = \left\{(\alpha, \beta) \in \mathbf{F}_q^2 \ ; \ \beta^2 = \alpha^6 - 1, \ \left(\frac{\alpha}{\mathfrak{p}}\right)_2 = 1\right\},$$

$$S = \left\{(\alpha, \beta) \in \mathbf{F}_q^2 \ ; \ \beta^2 = \alpha^6 - 1, \ \left(\frac{\alpha}{\mathfrak{p}}\right)_2 = -1\right\},$$

$$T = \left\{(\alpha, \beta) \in \mathbf{F}_q^2 \ ; \ \beta^2 = \alpha^6 - 1, \ \left(\frac{\alpha}{\mathfrak{p}}\right)_2 = 0\right\}$$

and

$$r = \#R\,, \quad s = \#S\,, \quad t = \#T\,.$$

Then we have

$$X(\mathbf{F}_q) - \{\infty_+, \infty_-\} = R \cup S \cup T$$

and

$$\#X(\mathbf{F}_q) - 2 = r + s + t\,,$$

where X is the hyperelliptic curve over $\mathbf{F}_q$ defined by the affine equation $y^2 = x^6 - 1$. This implies that

$$\sum_{\substack{(\alpha,\beta)\in\mathbf{F}_q^2 \\ \beta^2=\alpha^6-1}} \left(\frac{\beta}{\mathfrak{p}}\right)_2 = r - s = 2r + t - \#X(\mathbf{F}_q) + 2\,.$$

Hence we obtain the result from (a) $r \equiv 6 \mod 12$; (b) $t = 2$ and

$$(c)\ \#X(\mathbf{F}_q) \equiv \begin{cases} -2 \mod 24 & \text{if } q \equiv 1 \mod 24\,, \\ 10 \mod 24 & \text{if } q \equiv 13 \mod 24\,. \end{cases}$$

For the assertion of (a), we denote by ζ_6 a primitive 6th root of unity in $\mathbf{F}_q^\times$. Then we have $\left(\frac{\zeta_6}{\mathfrak{p}}\right)_2 = 1$ since $q \equiv 1 \mod 12$. This implies that

$$R = \left\{(\alpha, \beta) \in (\mathbf{F}_q^\times)^2 \ ; \ \beta^2 = \alpha^6 - 1, \ \left(\frac{\alpha}{\mathfrak{p}}\right)_2 = 1\right\} \cup \{(\pm 1, 0), (\pm\zeta_6, 0), (\pm\zeta_6^2, 0)\}\,.$$

Moreover the group $\boldsymbol{\mu}_6 \times \boldsymbol{\mu}_2$ acts faithfully on $R - \{(\pm 1, 0), (\pm\zeta_6, 0), (\pm\zeta_6^2, 0)\}$ by $(\xi, \theta)(\alpha, \beta) = (\xi\alpha, \theta\beta)$ since $\left(\frac{\zeta_6\alpha}{\mathfrak{p}}\right)_2 = \left(\frac{\alpha}{\mathfrak{p}}\right)_2$ for each $\alpha \in \mathbf{F}_q$.

It is easy to verify (b). In fact, there exist exactly two elements $\alpha \in \mathbf{F}_q^\times$ such that $\beta^2 = -1$ since $q \equiv 1 \mod 4$. The assertion (c) follows from Corollary 2.9 and 2.10.

3.8. Proof of Theorem 3.5. We have a prime factorization

$$(p) = (\pi, \rho)(\pi, \bar{\rho})(\bar{\pi}, \rho)(\bar{\pi}, \bar{\rho})$$

in $\mathbf{Q}(\zeta)=\mathbf{Q}(\sqrt{-1},\sqrt{-3})$.

By the definition, the Jacobi sum $J(\chi,\eta)$ is an integer in $\mathbf{Q}(\zeta)$. Furthermore we have a prime factorization

$$(J(\chi,\eta))=(\bar{\pi},\rho)(\pi,\rho)\,,$$

applying Stickelberger's theorem to $n=12$, $i=1$, $j=6$, $\mathfrak{p}=(\pi,\rho)$ and noting that

$$\begin{aligned}w(1,6)=&\left[\left\langle\frac{1}{12}\right\rangle+\left\langle\frac{6}{12}\right\rangle-\left\langle\frac{7}{12}\right\rangle\right]\sigma_{-1}^{-1}+\left[\left\langle\frac{5}{12}\right\rangle+\left\langle\frac{30}{12}\right\rangle-\left\langle\frac{35}{12}\right\rangle\right]\sigma_{-5}^{-1}\\&+\left[\left\langle\frac{7}{12}\right\rangle+\left\langle\frac{42}{12}\right\rangle-\left\langle\frac{49}{12}\right\rangle\right]\sigma_{-7}^{-1}+\left[\left\langle\frac{11}{12}\right\rangle+\left\langle\frac{66}{12}\right\rangle-\left\langle\frac{77}{12}\right\rangle\right]\sigma_{-11}^{-1}\\=&\,\sigma_5+\sigma_1\end{aligned}$$

and $\sigma_5(\pi)=\bar{\pi}$, $\sigma_5(\rho)=\rho$. This implies that

$$(J(\chi,\eta))=(\rho)\,.$$

Hence we can conclude that

$$J(\chi,\eta)\in\{\pm\rho,\pm\zeta\rho,\pm\zeta^2\rho,\pm\zeta^3\rho,\pm\zeta^4\rho,\pm\zeta^5\rho\}$$

since $|J(\chi,\eta)|=\sqrt{p}$ and $|\rho|=\sqrt{p}$.

In the case $p\equiv 1 \mod 24$, by Corollary 3.7, we have

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(J(\chi,\chi^6))+\mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}(J(\chi^3,\chi^6))\equiv -6 \mod 24\,.$$

Furthermore we have

$$\mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})}(J(\chi^3,\chi^6))=-2C$$

since $J(\chi^3,\chi^6)=-\rho$ as is shown in Example 1.9. Hence we obtain

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(J(\chi,\chi^6))-2C\equiv -6 \mod 24\,.$$

On the other hand, we have

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\rho)=4C\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta\rho)=-2D\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^2\rho)=2C\,,$$
$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^3\rho)=-4D\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^4\rho)=-2C\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^5\rho)=-2D\,,$$

and therefore

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\rho)-2C=2C\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta\rho)+-2C=-2C-2D\,,$$
$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^2\rho)-2C=0\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^3\rho)-2C=-2C-4D\,,$$
$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^4\rho)-2C=-4C\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^5\rho)-2C=-2C-2D$$

and

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\rho)-2C=-6C\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta\rho)-2C=-2C+2D\,,$$

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^2\rho) - 2C = -4C\,, \quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^3\rho) - 2C = -2C + 4D\,,$$
$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^4\rho) - 2C = 0\,, \quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^5\rho) - 2C = -2C + 2D\,.$$

Hence we obtain

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\rho) - 2C \equiv 2 \mod 8\,, \quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta\rho) - 2C \equiv -2 \mod 8\,,$$
$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^2\rho) - 2C = 0\,, \quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^3\rho) - 2C \equiv -2 \mod 8\,,$$
$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^4\rho) - 2C \equiv 4 \mod 8\,, \quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^5\rho) - 2C \equiv -2 \mod 8$$

and

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\rho) - 2C \equiv -6 \mod 24\,, \quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta\rho) - 2C \equiv -2 \mod 8\,,$$
$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^2\rho) - 2C \equiv 4 \mod 8\,, \quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^3\rho) - 2C \equiv -2 \mod 8\,,$$
$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^4\rho) - 2C = 0\,, \quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^5\rho) - 2C \equiv -2 \mod 8$$

since $C \equiv 1 \mod 4$, $D \equiv 0 \mod 4$.

Then we can conclude

$$J(\chi, \chi^6) = \rho \text{ or } -\rho\,.$$

If $C \not\equiv 0 \mod 3$, then we obtain

$$J(\chi, \chi^6) = -\rho\,.$$

since we have

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\rho) - 2C \not\equiv 0 \mod 6\,, \quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\rho) - 2C \equiv 0 \mod 6\,.$$

If $C \equiv 0 \mod 3$, which implies $D \not\equiv 0 \mod 3$, then we obtain

$$J(\chi, \chi^6) = \rho$$

from the observation below.

Take $a \in \mathbf{F}_p$ such that $\chi(a) = \zeta^3$ and put

$$R = \left\{(\alpha, \beta) \in \mathbf{F}_p^2\,;\ \beta^2 = \alpha^6 + a,\ \left(\frac{\alpha}{p}\right) = 1\right\},$$
$$S = \left\{(\alpha, \beta) \in \mathbf{F}_p^2\,;\ \beta^2 = \alpha^6 + a,\ \left(\frac{\alpha}{p}\right) = -1\right\},$$
$$T = \left\{(\alpha, \beta) \in \mathbf{F}_p^2\,;\ \beta^2 = \alpha^6 + a,\ \left(\frac{\alpha}{p}\right) = 0\right\}$$

and

$$r = \#R\,, \quad s = \#S\,, \quad t = \#T\,.$$

Then we have

$$X(\mathbf{F}_p) - \{\infty_+, \infty_-\} = R \cup S \cup T$$

and

$$\# X(\mathbf{F}_p) - 2 = r + s + t\,,$$

where X is the hyperelliptic curve over $\mathbf{F}_p$ defined by the affine equation $y^2 = x^6 + a$. This implies that

$$\sum_{\substack{(\alpha,\beta)\in\mathbf{F}_p^2 \\ \beta^2=\alpha^6+a}} \left(\frac{\alpha}{\pi,\rho}\right)_2 = r - s = 2r + t - \# X(\mathbf{F}_p) + 2\,.$$

Hence we obtain the result from (a) $r \equiv 0 \mod 12$; (b) $t = 0$; (c) $\# X(\mathbf{F}_p) \equiv 2 \mod 24$.

For the assertion of (a), note that

$$R = \left\{(\alpha,\beta) \in (\mathbf{F}_p^\times)^2\,;\ \beta^2 = \alpha^6 + a,\ \left(\frac{\alpha}{p}\right) = 1\right\}$$

since $\chi^2(-a) = -1$. Hence the group $\boldsymbol{\mu}_6 \times \boldsymbol{\mu}_2$ acts faithfully on R by $(\xi,\theta)(\alpha,\beta) = (\xi\alpha, \theta\beta)$ since $\left(\frac{\zeta_6\alpha}{\pi,\rho}\right)_2 = \left(\frac{\alpha}{\mathfrak{p}}\right)_2$ for each $\alpha \in \mathbf{F}_p$, where ζ_6 denotes a primitive 6th root of unity in $\mathbf{F}_p^\times$.

It is easy to verify (b). In fact, there exists no element $\alpha \in \mathbf{F}_p^\times$ such that $\beta^2 = -1$ since $\chi^6(a) = -1$. The assertion (c) follows from $\# X(\mathbf{F}_p) = p + 1$, which we obtain since $\chi^4(a) = 1$ and $\chi^6(a) = -1$ as is shown Proposition 2.1 and Example 1.6.

Hence we obtain

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^3 J(\chi,\chi^6)) + \mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}(\zeta^3 J(\chi^3,\chi^6)) \equiv 0 \mod 24$$

as is shown in the proof of Lemma 3.6 and Corollary 3.7. Furthermore we have

$$\mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}(\zeta^3 J(\chi^3,\chi^6)) = 2D$$

since $J(\chi^3,\chi^6) = -\rho$ as is shown in Example 1.9. Hence we obtain

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^3 J(\chi,\chi^6)) + 2D \equiv 0 \mod 24$$

On the other hand, we have

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^3\rho) = 4D\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^3(-\rho)) = -4D\,,$$

and therefore

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^3\rho) + 2D = 6D\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^3(-\rho)) + 2D = -2D\,.$$

Hence we obtain

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^3\rho) + 2D \equiv 0 \mod 6\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^3(-\rho)) + 2D \not\equiv 0 \mod 6\,.$$

Therefore we obtain

$$J(\chi,\chi^6)=\rho\,.$$

In the case $p\equiv 13 \mod 24$, by Corollary 3.7, we have

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(J(\chi,\chi^6))+\mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}(J(\chi^3,\chi^6))\equiv 6 \mod 24\,.$$

Furthermore we have

$$\mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}(J(\chi^3,\chi^6))=2C$$

since $J(\chi^3,\chi^6)=\rho$ as is shown in Example 1.9. Hence we obtain

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(J(\chi,\chi^6))+2C\equiv 6 \mod 24\,.$$

On the other hand, we have

$$\begin{gathered}\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\rho)+2C=6C\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta\rho)+2C=2C-2D\,,\\ \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^2\rho)+2C=4C\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^3\rho)+2C=2C-4D\,,\\ \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^4\rho)+2C=0\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^5\rho)+2C=2C-2D\end{gathered}$$

and

$$\begin{gathered}\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\rho)+2C=-2C\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta\rho)+2C=2C+2D\,,\\ \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^2\rho)+2C=0\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^3\rho)+2C=2C+4D\,,\\ \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^4\rho)+2C=4C\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^5\rho)+2C=2C+2D\,.\end{gathered}$$

Hence we obtain

$$\begin{gathered}\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\rho)+2C\equiv 6 \mod 24\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta\rho)+2C\equiv -2 \mod 8\,,\\ \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^2\rho)+2C\equiv 4 \mod 8\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^3\rho)+2C\equiv 2 \mod 8\,,\\ \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^4\rho)+2C=0\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^5\rho)+2C\equiv -2 \mod 8\end{gathered}$$

and

$$\begin{gathered}\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\rho)+2C\equiv -2 \mod 8\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta\rho)+2C\equiv -2 \mod 8\,,\\ \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^2\rho)+2C=0\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^3\rho)+2C\equiv 2 \mod 8\,,\\ \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^4\rho)+2C\equiv 4 \mod 8\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^5\rho)+2C\equiv -2 \mod 8\end{gathered}$$

since $C\equiv 1 \mod 4$ and $D\equiv 2 \mod 4$.

These imply that

$$J(\chi,\chi^6)\in\{\pm\rho,\pm\zeta\rho,\pm\zeta^5\rho\}\,.$$

Furthermore we have

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta\rho)+2C\not\equiv 0 \mod 6\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^5\rho)+2C\not\equiv 0 \mod 6$$

and

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta\rho)+2C\not\equiv 0 \mod 6\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^5\rho)+2C\not\equiv 0 \mod 6$$

since $C+D\not\equiv 0 \mod 3$ and $C-D\not\equiv 0 \mod 3$.

Then we can conclude that

$$J(\chi,\chi^6)\in\{\pm\rho\}\,.$$

If $C\not\equiv 0 \mod 3$, then we obtain

$$J(\chi,\chi^6)=\rho\,.$$

since we have

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\rho)+2C\equiv 0 \mod 6\,,\quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\rho)+2C\not\equiv 0 \mod 6\,.$$

If $C\equiv 0 \mod 3$, which implies $D\not\equiv 0 \mod 3$, then we obtain

$$J(\chi,\chi^6)=-\rho\,.$$

from the observation below.

Take $a\in\mathbf{F}_p$ such that $\chi(a)=-\zeta^3$. Put

$$R=\left\{(\alpha,\beta)\in\mathbf{F}_p^2\,;\ \beta^2=\alpha^6+a,\ \left(\frac{\alpha}{p}\right)=1\right\},$$

$$S=\left\{(\alpha,\beta)\in\mathbf{F}_p^2\,;\ \beta^2=\alpha^6+a,\ \left(\frac{\alpha}{p}\right)=-1\right\},$$

$$T=\left\{(\alpha,\beta)\in\mathbf{F}_p^2\,;\ \beta^2=\alpha^6+a,\ \left(\frac{\alpha}{p}\right)=0\right\}$$

and

$$r=\#R\,,\quad s=\#S\,,\quad t=\#T\,.$$

Then we have

$$X(\mathbf{F}_p)-\{\infty_+,\infty_-\}=R\cup S\cup T$$

and

$$\#X(\mathbf{F}_p)-2=r+s+t\,,$$

where X is the hyperelliptic curve over $\mathbf{F}_p$ defined by the affine equation $y^2=x^6+a$. This implies that

$$\sum_{\substack{(\alpha,\beta)\in\mathbf{F}_p^2\\ \beta^2=\alpha^6+a}}\left(\frac{\alpha}{\pi,\rho}\right)_2=r-s=2r+t-\#X(\mathbf{F}_p)+2\,.$$

Hence we obtain the result from (a) $r \equiv 0 \mod 12$; (b) $t = 0$; (c) $\#X(\mathbf{F}_p) \equiv 14 \mod 24$.

For the assertion of (a), note that

$$R = \left\{ (\alpha, \beta) \in (\mathbf{F}_p^\times)^2 \,;\; \beta^2 = \alpha^6 + a,\; \left(\frac{\alpha}{p}\right) = 1 \right\}$$

since $\chi^2(-a) = -1$. Hence the group $\boldsymbol{\mu}_6 \times \boldsymbol{\mu}_2$ acts faithfully on R by $(\xi, \theta)(\alpha, \beta) = (\xi\alpha, \theta\beta)$ since $\left(\frac{\zeta_6\alpha}{\pi, \rho}\right)_2 = \left(\frac{\alpha}{\mathfrak{p}}\right)_2$ for each $\alpha \in \mathbf{F}_p$, where ζ_6 denotes a primitive 6th root of unity in $\mathbf{F}_p^\times$.

It is easy to verify (b). In fact, there exists no element $\alpha \in \mathbf{F}_p^\times$ such that $\beta^2 = -1$ since $\chi^6(a) = -1$. The assertion (c) follows from $\#X(\mathbf{F}_p) = p + 1$, which we obtain since $\chi^4(a) = 1$ and $\chi^6(a) = -1$ as is shown in Proposition 2.1.

Hence we obtain

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^3 J(\chi, \chi^6)) + \mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}(\zeta^3 J(\chi^3, \chi^6)) \equiv 12 \mod 24$$

as is shown in the proof of Lemma 3.6 and Corollary 3.7. Furthermore we have

$$\mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}(\zeta^3 J(\chi^3, \chi^6)) = -2D$$

since we have $J(\chi^3, \chi^6) = \rho$ as is shown in Example 1.9. Hence we obtain

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^3 J(\chi, \chi^6)) - 2D \equiv 12 \mod 24$$

On the other hand, we obtain

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^3 \rho) = 4D\,, \quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^3(-\rho)) = -4D$$

and therefore

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^3 \rho) - 2D = 2D\,, \quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^3(-\rho)) - 2D = -6D\,.$$

Hence we have

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^3 \rho) - 2D \not\equiv 0 \mod 6\,, \quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta^3(-\rho)) - 2D \equiv 0 \mod 6\,.$$

These imply that

$$J(\chi, \chi^6) = -\rho\,.$$

4. Congruence zeta function of the curve $y^2 = x^{12} + a$

Throughout the section, we put $\zeta = e^{\pi i/6}$.

4.1. Let p be a prime number which is prime to 6. Let Y and X denote the hyperelliptic curves defined by the affine equation $y^2 = x^{12} + a$ and by the affine equation $y^2 = x^6 + a$ over $\mathbf{F}_p$, respectively. Moreover let $\tilde{E}$ denote the elliptic curve defined by the affine equation $y^2 = x^4 + a$ over $\mathbf{F}_p$. Let $J(Y)$ and $J(X)$ denote the Jacobian varieties of Y and X, respectively.

Then the double covering $Y \to X$ defined by $(x, y) \mapsto (x^2, y)$ and the triple covering $Y \to \tilde{E}$ defined by $(x, y) \mapsto (x^3, y)$ induce a homomorphism of abelian varieties $J(X) \times \tilde{E} \to J(Y)$. Put $S = \mathrm{Coker}[J(X) \times \tilde{E} \to J(Y)]$. Then S is an abelian surface over $\mathbf{F}_p$, and $J(Y)$ is isogenous to the product $J(X) \times \tilde{E} \times S$.

Let $P(J(Y)/\mathbf{F}_p; t)$, $P(J(X)/\mathbf{F}_p; t)$, $P(\tilde{E}/\mathbf{F}_p; t)$ and $P(S/\mathbf{F}_p; t)$ denote the characteristic polynomials of the Frobenius on $J(Y)$, $J(X)$, $\tilde{E}$ and S over $\mathbf{F}_p$, respectively. Then we have

$$(1-t)(1-pt)Z(Y/\mathbf{F}_p; t) = P(J(Y)/\mathbf{F}_p; t)$$

and

$$P(J(Y)/\mathbf{F}_p; t) = P(J(X)/\mathbf{F}_p; t)P(\tilde{E}/\mathbf{F}_p; t)P(S/\mathbf{F}_p; t)\,.$$

THEOREM 4.2. *Under the notations of* 4.1, *we put* $P(t) = P(S/\mathbf{F}_p, t)$. Then:

(1) *Suppose* $p \equiv 1 \mod 12$. *There exist uniquely pairs of integers* (A, B) *and* (C, D) *with*

$$A^2 + 3B^2 = p\,, \quad A \equiv 1 \mod 3\,, \quad B > 0$$

and

$$C^2 + D^2 = p\,, \quad C \equiv 1 \mod 4\,, \quad D > 0\,.$$

Put $\pi = A + B\sqrt{-3}$ *and* $\rho = C + D\sqrt{-1}$, *and let* χ *denote the multiplicative character of* $\mathbf{F}_p$ *defined by* $\alpha \mapsto \left(\frac{\alpha}{\pi,\rho}\right)_{12}$. *Furthermore we put* $\varepsilon = \pm 1$.

Suppose $C \not\equiv 0 \mod 3$. *Then we have*:

(a) $P(t) = (1 - \varepsilon 2Ct + pt^2)^2$ *if* $\chi(a) = \varepsilon$;

(b) $P(t) = (1 - \varepsilon 2Dt + pt^2)^2$ *if* $\chi(a) = \varepsilon\zeta^3$;

(c) $P(t) = 1 - \varepsilon 2Dt + (-C^2 + 3D^2)t^2 - \varepsilon 2Dpt^3 + p^2t^4$ *if* $\chi(a) = \varepsilon\zeta$;

(d) $P(t) = 1 + \varepsilon 2Ct + (3C^2 - D^2)t^2 + \varepsilon 2Cpt^3 + p^2t^4$ *if* $\chi(a) = \varepsilon\zeta^4$ *or* $-\varepsilon\zeta^2$;

(e) $P(t) = 1 - \varepsilon 2Dt + (-C^2 + 3D^2)t^2 - \varepsilon 2Dpt^3 + p^2t^4$ *if* $\chi(a) = \varepsilon\zeta^5$.

Suppose $C \equiv 0 \mod 3$. *Then we have*:

(a) $P(t) = (1 + \varepsilon 2Ct + pt^2)^2$ *if* $\chi(a) = \varepsilon$;

(b) $P(t) = (1 + \varepsilon 2Dt + pt^2)^2$ *if* $\chi(a) = \varepsilon\zeta^3$;

(c) $P(t) = 1 + \varepsilon 2Dt + (-C^2 + 3D^2)t^2 + \varepsilon 2Dpt^3 + p^2t^4$ *if* $\chi(a) = \varepsilon\zeta$;

(d) $P(t) = 1 - \varepsilon 2Ct + (3C^2 - D^2)t^2 - \varepsilon 2Cpt^3 + p^2t^4$ *if* $\chi(a) = \varepsilon\zeta^4$ *or* $-\varepsilon\zeta^2$;

(e) $P(t) = 1 + \varepsilon 2Dt + (-C^2 + 3D^2)t^2 + \varepsilon 2Dpt^3 + p^2t^4$ *if* $\chi(a) = \varepsilon\zeta^5$.

(2) *Suppose* $p \equiv 5 \mod 12$. *There exists uniquely a pair of integers* (C, D) *with*

$$C^2 + D^2 = p\,, \quad C \equiv 1 \mod 4\,, \quad D > 0\,.$$

Then we have:

(a) $P(t) = (1 + 2Dt + pt^2)(1 - 2Dt + pt^2)$ *if* $(\frac{a}{p}) = 1$;

(b) $P(t) = (1 + 2Ct + pt^2)(1 - 2Ct + pt^2)$ *if* $\left(\frac{a}{p}\right) = -1$.

(3) *Suppose* $p \equiv 7 \mod 12$. *There exists uniquely a pair of integers* (A, B) *with*

$$A^2 + 3B^2 = p\,, \quad A \equiv 1 \mod 3\,, \quad B > 0\,.$$

Put $\pi = A + B\sqrt{-3}$, *and let* χ *denote the multiplicative character of* $\mathbf{F}_p$ *defined by* $\alpha \mapsto \left(\frac{\alpha}{\pi}\right)_3$. *Then we have*:

(a) $P(t) = (1 + pt^2)^2$ *if* $\chi(a) = 1$;

(b) $P(t) = 1 - pt^2 + p^2t^4$ *if* $\chi(a) \neq 1$.

(4) *Suppose* $p \equiv 11 \mod 12$. *Then we have* $P(t) = (1 + pt^2)^2$.

4.3. Proof of (1). By the theorem of Davenport-Hasse and 4.1, we have

$$P(t) = \prod_{\substack{0<i<12\\(i,12)=1}} (1 + \chi(-1)\chi^{i+6}(a)J(\chi^i, \chi^6)\,t)\,.$$

Furthermore, if $C \not\equiv 0 \mod 3$, then we have

$$\chi(-1)J(\chi, \chi^6) = \chi(-1)J(\chi^5, \chi^6) = -(C + D\sqrt{-1})\,,$$

$$\chi(-1)J(\chi^7, \chi^6) = \chi(-1)J(\chi^{11}, \chi^6) = -(C - D\sqrt{-1})$$

and, if $C \equiv 0 \mod 3$, then we have

$$\chi(-1)J(\chi, \chi^6) = \chi(-1)J(\chi^5, \chi^6) = C + D\sqrt{-1}\,,$$

$$\chi(-1)J(\chi^7, \chi^6) = \chi(-1)J(\chi^{11}, \chi^6) = C - D\sqrt{-1}$$

as is proved in Theorem 3.5. Hence we obtain the result, expanding the right hand side in each case.

4.4. Proof of (3). First note that the prime ideals (π) and $(\bar{\pi})$ of $\mathbf{Q}(\sqrt{-3})$ inert in the extension $\mathbf{Q}(\zeta)/\mathbf{Q}(\sqrt{-3})$, and we have a prime factorization $(p) = (\pi)(\bar{\pi})$ in $\mathbf{Q}(\zeta)$. Let $\tilde{\chi}$ denote the multiplicative character of $\mathbf{F}_{p^2}$ defined by $\alpha \mapsto \left(\frac{\alpha}{\pi}\right)_{12}$.

By the definition, the Jacobi sum $J(\tilde{\chi}, \tilde{\chi}^6)$ is an integer in $\mathbf{Q}(\zeta)$. We have a prime factorization

$$(J(\tilde{\chi}, \tilde{\chi}^6)) = (\bar{\pi})(\pi)\,,$$

applying Stickelberger's theorem to $n = 12$, $i = 1$, $j = 6$, $\mathfrak{p} = (\pi)$ and noting that

$$w(1, 6) = \sigma_5 + \sigma_1$$

and $\sigma_5(\pi) = \bar{\pi}$ as is shown in 3.8.

This implies that

$$(J(\tilde{\chi}, \tilde{\chi}^6)) = (p)\,.$$

Hence we can conclude that

$$J(\tilde{\chi}, \tilde{\chi}^6) \in \{\pm p, \pm\zeta p, \pm\zeta^2 p, \pm\zeta^3 p, \pm\zeta^4 p, \pm\zeta^5 p\}$$

since $|J(\tilde{\chi}, \tilde{\chi}^6)| = p$.

By Corollary 3.7, we have

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(J(\tilde{\chi}, \tilde{\chi}^6)) + \mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}(J(\tilde{\chi}^3, \tilde{\chi}^6)) \equiv -6 \mod 24\,,$$

and furthermore we have

$$\mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}(J(\tilde{\chi}^3, \tilde{\chi}^6)) = 2p$$

since $J(\tilde{\chi}, \tilde{\chi}^6) = p$ by Remark 1.10. Hence we obtain

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(J(\tilde{\chi}, \tilde{\chi}^6)) \equiv 4 \mod 24\,.$$

On the other hand, we have

$$\mathrm{Tr}(p) = 4p\,,\quad \mathrm{Tr}(\zeta p) = \mathrm{Tr}(\zeta^3 p) = \mathrm{Tr}(\zeta^5 p) = 0\,,\quad \mathrm{Tr}(\zeta^2 p) = 2p\,,\quad \mathrm{Tr}(\zeta^4 p) = -2p$$

and therefore

$$\mathrm{Tr}(p) \equiv 4 \mod 24\,,\quad \mathrm{Tr}(-p) \equiv -4 \mod 16\,,\quad \mathrm{Tr}(\zeta^2 p) = \mathrm{Tr}(-\zeta^4 p) \equiv 14 \mod 24\,,$$
$$\mathrm{Tr}(-\zeta^2 p) = \mathrm{Tr}(\zeta^4 p) \equiv -14 \mod 24$$

since $p \equiv 7 \mod 12$. These imply that

$$J(\tilde{\chi}, \tilde{\chi}^6) = J(\tilde{\chi}^5, \tilde{\chi}^6) = J(\tilde{\chi}^7, \tilde{\chi}^6) = J(\tilde{\chi}^{11}, \tilde{\chi}^6) = p\,.$$

Let now $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ and β_1, β_2 denote the eigenvalues of the Frobenius on the abelian varieties $S = \mathrm{Coker}[J(X) \times \tilde{E} \to J(Y)]$ and $\tilde{E}$ over $\mathbf{F}_p$, respectively. Then we have $\{\beta_1, \beta_2\} = \{\sqrt{-p}, -\sqrt{-p}\}$ as is shown in Remark 1.10 since $p \equiv 3 \mod 4$. For any $a \in \mathbf{F}_p$, we have $\tilde{\chi}(a) = \chi^2(a)$ since $p + 1 \equiv 8 \mod 12$. Hence, if $\chi(a) = 1$, we have

$$\begin{aligned}\{\alpha_1^2, \alpha_2^2, \alpha_3^2, \alpha_4^2\} &= \{-J(\tilde{\chi}, \tilde{\chi}^6), -J(\tilde{\chi}^5, \tilde{\chi}^6), -J(\tilde{\chi}^7, \tilde{\chi}^6), -J(\tilde{\chi}^{11}, \tilde{\chi}^6)\}\\ &= \{-p, -p, -p, -p\}\,,\end{aligned}$$

and therefore

$$\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} = \{\sqrt{-p}, -\sqrt{-p}, \sqrt{-p}, -\sqrt{-p}\}\,.$$

Hence we obtain

$$P(S/\mathbf{F}_p; t) = (1 + pt^2)^2\,.$$

If $\chi(a) = \zeta^4$, then we obtain

$$\{\alpha_1^2, \alpha_2^2, \alpha_3^2, \alpha_4^2\} = \{-\zeta^8 J(\tilde{\chi}, \tilde{\chi}^6), -\zeta^4 J(\tilde{\chi}^5, \tilde{\chi}^6), -\zeta^8 J(\tilde{\chi}^7, \tilde{\chi}^6), -\zeta^4 J(\tilde{\chi}^{11}, \tilde{\chi}^6)$$

$$= \{-\zeta^8 p, -\zeta^4 p, -\zeta^8 p, -\zeta^4 p\}\,.$$

We have $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$ since $\#Y(\mathbf{F}_p) = \#X(\mathbf{F}_p)$ as is shown in 3.3, and $\beta_1 + \beta_2 = 0$. Therefore we obtain

$$\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} = \{\zeta\sqrt{p}, \zeta^5\sqrt{p}, -\zeta\sqrt{p}, -\zeta^5\sqrt{p}\}\,.$$

This implies that

$$P(S/\mathbf{F}_p; t) = 1 - pt^2 + p^2t^4\,.$$

If $\chi(a) = \zeta^8$, then we obtain

$$\begin{aligned}\{\alpha_1^2, \alpha_2^2, \alpha_3^2, \alpha_4^2\} &= \{-\zeta^4 J(\tilde{\chi}, \tilde{\chi}^6), -\zeta^8 J(\tilde{\chi}^5, \tilde{\chi}^6), -\zeta^4 J(\tilde{\chi}^7, \tilde{\chi}^6), -\zeta^8 J(\tilde{\chi}^{11}, \tilde{\chi}^6)\}\\ &= \{-\zeta^4 p, -\zeta^8 p, -\zeta^4 p, -\zeta^8 p\}\,.\end{aligned}$$

Hence we obtain

$$P(S/\mathbf{F}_p; t) = 1 - pt^2 + p^2t^4$$

as above.

4.5. Proof of (4). We have a prime factorization $(p) = \mathfrak{q}\mathfrak{q}'$ in $\mathbf{Q}(\sqrt{3})$ $(\mathfrak{q} \neq \mathfrak{q}')$ since $p \equiv 11 \mod 12$. Moreover the prime ideals $\mathfrak{q}$ and $\mathfrak{q}'$ inert in the extension $\mathbf{Q}(\zeta)/\mathbf{Q}(\sqrt{3})$, and we have a prime factorization $(p) = \mathfrak{q}\mathfrak{q}'$ in $\mathbf{Q}(\zeta)$. Let χ denote the multiplicative character of $\mathbf{F}_{p^2}$ defined by $\alpha \mapsto \left(\frac{\alpha}{\mathfrak{q}}\right)_{12}$.

By the definition, the Jacobi sum $J(\chi, \chi^6)$ is an integer in $\mathbf{Q}(\zeta)$. We obtain a prime factorization

$$(J(\chi, \chi^6)) = \mathfrak{q}'\mathfrak{q}\,,$$

applying Stickelberger's theorem to $n = 12$, $i = 1$, $j = 6$, $\mathfrak{p} = \mathfrak{q}$ and noting that

$$w(1, 6) = \sigma_5 + \sigma_1$$

and $\sigma_5(\mathfrak{q}) = \mathfrak{q}'$.

This implies that

$$(J(\chi, \chi^6)) = (p)\,.$$

Hence we can conclude that

$$J(\chi, \chi^6) \in \{\pm p, \pm\zeta p, \pm\zeta^2 p, \pm\zeta^3 p, \pm\zeta^4 p, \pm\zeta^5 p\}$$

since $|J(\chi, \chi^6)| = p$.

By Corollary 3.7, we have

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(J(\chi, \chi^6)) + \mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}(J(\chi^3, \chi^6)) \equiv -6 \mod 24\,,$$

and furthermore we have

$$\mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}(J(\chi^3,\chi^6)) = 2p$$

since $J(\chi^3,\chi^6) = p$ by Remark 1.10. Hence we obtain

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(J(\chi,\chi^6)) \equiv -4 \mod 24\,.$$

On the other hand, we have

$$\mathrm{Tr}(p) = 4p\,,\quad \mathrm{Tr}(\zeta p) = \mathrm{Tr}(\zeta^3 p) = \mathrm{Tr}(\zeta^5 p) = 0\,,\quad \mathrm{Tr}(\zeta^2 p) = 2p\,,\quad \mathrm{Tr}(\zeta^4 p) = -2p$$

and therefore

$$\mathrm{Tr}(p) \equiv -4 \mod 24\,,\quad \mathrm{Tr}(-p) \equiv 4 \mod 24\,,\quad \mathrm{Tr}(\zeta^2 p) = \mathrm{Tr}(-\zeta^4 p) \equiv -2 \mod 24\,,$$

$$\mathrm{Tr}(-\zeta^2 p) = \mathrm{Tr}(\zeta^4 p) \equiv 2 \mod 24$$

since $p \equiv 11 \mod 12$. These imply that

$$J(\chi,\chi^6) = J(\chi^5,\chi^6) = J(\chi^7,\chi^6) = J(\chi^{11},\chi^6) = p\,.$$

Let now $\alpha_1,\alpha_2,\alpha_3,\alpha_4$ and β_1,β_2 denote the eigenvalues of the Frobenius on the abelian varieties $S = \mathrm{Coker}[J(X)\times\tilde{E} \to J(Y)]$ and $\tilde{E}$ over $\mathbf{F}_p$, respectively. Then we have $\{\beta_1,\beta_2\} = \{\sqrt{-p},-\sqrt{-p}\}$ as is shown in Remark 1.10 since $p \equiv 3 \mod 4$. For any $a \in \mathbf{F}_p$, we have $\chi(a) = 1$ since $p+1 \equiv 0 \mod 12$. Hence, we have

$$\begin{aligned}\{\alpha_1^2,\alpha_2^2,\alpha_3^2,\alpha_4^2\} &= \{-J(\chi,\chi^6),-J(\chi^5,\chi^6),-J(\chi^7,\chi^6),-J(\chi^{11},\chi^6)\}\\ &= \{-p,-p,-p,-p\}\,.\end{aligned}$$

Here, we obtain $\alpha_1+\alpha_2+\alpha_3+\alpha_4 = 0$ since $\#Y(\mathbf{F}_p) = \#X(\mathbf{F}_p)$ as is shown in 3.3, and $\beta_1+\beta_2 = 0$. Therefore we obtain

$$\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\} = \{\sqrt{-p},-\sqrt{-p},\sqrt{-p},-\sqrt{-p}\}\,.$$

Hence we have

$$P(S/\mathbf{F}_p;t) = (1+pt^2)^2\,.$$

4.6. Proof of (2). First note that the prime ideals (ρ) and $(\bar{\rho})$ of $\mathbf{Q}(\sqrt{-1})$ inert in the extension $\mathbf{Q}(\zeta)/\mathbf{Q}(\sqrt{-1})$, and we have a prime factorization $(p) = (\rho)(\bar{\rho})$ in $\mathbf{Q}(\zeta)$. Let χ denote the multiplicative character of $\mathbf{F}_{p^2}$ defined by $\alpha \mapsto \left(\frac{\alpha}{\rho}\right)_{12}$.

By the definition, the Jacobi sum $J(\chi,\chi^6)$ is an integer in $\mathbf{Q}(\zeta)$. We obtain a prime factorization

$$(J(\chi,\chi^6)) = (\rho^2)\,,$$

applying Stickelberger's theorem to $n = 12$, $i = 1$, $j = 6$, $\mathfrak{p} = (\rho)$ and noting that

$$w(1,6) = \sigma_5 + \sigma_1$$

and $\sigma_5(\rho) = \rho$.

Hence we can conclude that

$$J(\chi, \chi^6) \in \{\pm\rho^2, \pm\zeta\rho^2, \pm\zeta^2\rho^2, \pm\zeta^3\rho^2, \pm\zeta^4\rho^2, \pm\zeta^5\rho^2\}$$

since $|J(\chi, \chi^6)| = |\rho^2| = p$.

By Corollary 3.7, we have

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(J(\chi, \chi^6)) + \mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}(J(\chi^3, \chi^6)) \equiv -6 \mod 24\,.$$

Furthermore we have

$$J(\chi^3, \chi^6) = -\rho^2$$

since $J(\chi^3, \chi^6) = -\rho^2$ as is shown in Remark 1.10, and therefore

$$\mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}(J(\chi^3, \chi^6)) = -2(C^2 - D^2) = -4C^2 + 2p \equiv 6 \mod 24$$

since $C^2 \equiv 1 \mod 6$. These imply that

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(J(\chi, \chi^6)) \equiv 12 \mod 24\,.$$

On the other hand, we have

$$\begin{gathered}
\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\rho^2) = 4(C^2 - D^2)\,, \quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta\rho^2) = -4CD\,,\\
\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^2\rho^2) = 2(C^2 - D^2)\,, \quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^3\rho^2) = -8CD\,,\\
\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^4\rho^2) = -2(C^2 - D^2)\,, \quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^5\rho^2) = -4CD
\end{gathered}$$

and therefore,

$$\begin{gathered}
\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\pm\rho^2) \equiv 12 \mod 24\,, \quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\pm\zeta\rho^2) \not\equiv 0 \mod 12\,,\\
\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\pm\zeta^2\rho^2) \equiv \mp 6 \mod 24\,, \quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\pm\zeta^3\rho^2) \not\equiv 0 \mod 12\,,\\
\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\pm\zeta^4\rho^2) \equiv \pm 6 \mod 24\,, \quad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\pm\zeta^5\rho^2) \not\equiv 0 \mod 12
\end{gathered}$$

since $C^2 - D^2 \equiv -3 \mod 12$ and $CD \not\equiv 0 \mod 3$.

Hence we obtain

$$J(\chi, \chi^6) \in \{\pm\rho^2\}\,.$$

In the next paragraph, we verify that

$$(\#) \qquad J(\chi, \chi^6) = \rho^2\,.$$

Admitting (#), we verify the assertion.

Let now $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ and $\beta_1, \beta_2, \beta_3, \beta_4$ denote the eigenvalues of the Frobenius on the abelian varieties $S = \mathrm{Coker}[J(X) \times \tilde{E} \to J(Y)]$ and $J(X)$ over $\mathbf{F}_p$, respectively. Then we have $\{\beta_1, \beta_2, \beta_3, \beta_4\} = \{\sqrt{-p}, -\sqrt{-p}, \sqrt{-p}, -\sqrt{-p}\}$ as is shown in Remark 1.7 and Corollary 2.8. Then we have

$$\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$$

since $\#Y(\mathbf{F}_p) = \#\tilde{E}(\mathbf{F}_p)$ as is shown in 3.2, and $\beta_1 + \beta_2 + \beta_3 + \beta_4 = 0$. For any $a \in \mathbf{F}_p$, we have $\chi(a) = \left(\frac{a}{p}\right)$ since $p + 1 \equiv 6 \mod 12$.

If $\chi(a) = 1$, we have

$$\begin{aligned}\{\alpha_1^2, \alpha_2^2, \alpha_3^2, \alpha_4^2\} &= \{-J(\chi, \chi^6), -J(\chi^5, \chi^6), -J(\chi^7, \chi^6), -J(\chi^{11}, \chi^6)\} \\ &= \{-\rho^2, -\rho^2, -\bar{\rho}^2, -\bar{\rho}^2\},\end{aligned}$$

and therefore

$$\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} = \{\sqrt{-1}\rho, -\sqrt{-1}\rho, -\sqrt{-1}\bar{\rho}, \sqrt{-1}\bar{\rho}.\}$$

This implies that

$$P(S/\mathbf{F}_p; t) = (1 + 2Dt + pt^2)(1 - 2Dt + pt^2).$$

If $\chi(a) = -1$, we have

$$\{\alpha_1^2, \alpha_2^2, \alpha_3^2, \alpha_4^2\} = \{J(\chi, \chi^6), J(\chi^5, \chi^6), J(\chi^7, \chi^6), J(\chi^{11}, \chi^6))\} = \{\rho^2, \rho^2, \bar{\rho}^2, \bar{\rho}^2\},$$

and therefore

$$\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} = \{\rho, -\rho, \bar{\rho}, -\bar{\rho}\}.$$

This implies that

$$P(S/\mathbf{F}_p; t) = (1 + 2Ct + pt^2)(1 - 2Ct + pt^2).$$

4.7. Proof of (#). Assume $J(\chi, \chi^6) = -\rho^2$. Take $a \in \mathbf{F}_{p^2}$ such that $\chi(a) = \zeta^3$. Then we obtain

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\chi^7(a)J(\chi, \chi^6)) + \mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}(\chi^9(a)J(\chi^3, \chi^6)) = -4CD$$

since $J(\chi^3, \chi^6) = -\rho^2$ as is shown in Remark 1.10. Hence we obtain

$$(*) \qquad \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\chi^7(a)J(\chi, \chi^6)) + \mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}(\chi^9(a)J(\chi^3, \chi^6)) \not\equiv 0 \mod 24$$

since $CD \not\equiv 0 \mod 3$.

On the other hand, we put

$$R = \left\{(\alpha, \beta) \in \mathbf{F}_{p^2}^2\,;\ \beta^2 = \alpha^6 + a,\ \left(\frac{\alpha}{\rho}\right)_2 = 1\right\},$$

$$S = \left\{(\alpha, \beta) \in \mathbf{F}_{p^2}^2\,;\ \beta^2 = \alpha^6 + a,\ \left(\frac{\alpha}{\rho}\right)_2 = -1\right\},$$

$$T = \left\{(\alpha, \beta) \in \mathbf{F}_{p^2}^2 \,;\; \beta^2 = \alpha^6 + a,\; \left(\frac{\alpha}{\rho}\right)_2 = 0\right\}$$

and

$$r = \#R\,, \quad s = \#S\,, \quad t = \#T\,.$$

Then we have

$$X(\mathbf{F}_{p^2}) - \{\infty_+, \infty_-\} = R \cup S \cup T$$

and

$$\#X(\mathbf{F}_{p^2}) - 2 = r + s + t\,,$$

where X is the hyperelliptic curve over $\mathbf{F}_{p^2}$ defined by the affine equation $y^2 = x^6 + a$. This implies that

$$\sum_{\substack{(\alpha,\beta)\in\mathbf{F}_{p^2}^2 \\ \beta^2=\alpha^6+a}} \left(\frac{\alpha}{\rho}\right)_2 = r - s = 2r + t - \#X(\mathbf{F}_{p^2}) + 2\,.$$

Then we obtain that (a) $r \equiv 0 \mod 12$; (b) $t = 0$; (c) $\#X(\mathbf{F}_{p^2}) \equiv 2 \mod 24$.

For the assertion of (a), note that

$$R = \left\{(\alpha, \beta) \in (\mathbf{F}_{p^2}^{\times})^2 \,;\; \beta^2 = \alpha^6 + a,\; \left(\frac{\alpha}{\rho}\right)_2 = 1\right\}$$

since $\chi^2(-a) = -1$. Moreover the group $\boldsymbol{\mu}_6 \times \boldsymbol{\mu}_2$ acts faithfully on R by $(\xi, \theta)(\alpha, \beta) = (\xi\alpha, \theta\beta)$ since $\left(\frac{\zeta_6\alpha}{\rho}\right)_2 = \left(\frac{\alpha}{\rho}\right)_2$ for each $\alpha \in \mathbf{F}_{p^2}$, where ζ_6 denotes a primitive 6th root of unity in $\mathbf{F}_{p^2}^{\times}$.

It is easy to verify (b). In fact, there exists no element $\beta \in \mathbf{F}_{p^2}^{\times}$ such that $\beta^2 = a$ since $\chi^6(a) = -1$.

For the assertion of (c), applying the theorem of Davenport-Hasse to X, we obtain

$$\begin{aligned}\#X(\mathbf{F}_{p^2}) = p^2 + 1 &+ \chi(-1)\chi^8(a)J(\chi^2, \chi^6) + \chi(-1)\chi^4(a)J(\chi^{10}, \chi^6) \\ &+ \chi(-1)\chi^{10}(a)J(\chi^4, \chi^6) + \chi(-1)\chi^2(a)J(\chi^8, \chi^6)\,.\end{aligned}$$

Furthermore we have $J(\chi, \chi^6) = J(\chi^4, \chi^6) = p$ as is shown in Corollary 2.8 and Remark 1.7, and $\chi^2(a) = -1$. These imply that $\#X(\mathbf{F}_{p^2}) = p^2 + 1$. Hence (c) follows.

These imply that

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\chi^7(a)J(\chi, \chi^6)) + \mathrm{Tr}_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}(\chi^9(a)J(\chi^3, \chi^6)) \equiv 0 \mod 24$$

as is in the proof of Lemma 3.6 and Corollary 3.7. This contradicts to $(*)$.

REMARK 4.8. Let p be a prime number which is prime to 6. Let Y and X denote the hyperelliptic curves defined by the affine equation $y^2 = x^{12} + 1$ and by the affine equation $y^2 = x^6 + 1$ over $\mathbf{F}_p$, respectively. Moreover let $\tilde{E}$ denote the elliptic curve defined by the affine equation $y^2 = x^4 + 1$ over $\mathbf{F}_p$. Put $S = \mathrm{Coker}[J(X) \times \tilde{E} \to J(Y)]$.

If $p \equiv 1 \mod 12$, then S is isogenous to the self-product of an ordinary elliptic curve with complex multiplication in $\mathbf{Q}(\sqrt{-1})$ over $\mathbf{F}_p$.

If $p \equiv 5 \mod 12$, then S is isogenous to the product of ordinary elliptic curves with complex multiplication in $\mathbf{Q}(\sqrt{-1})$ over $\mathbf{F}_p$.

If $p \equiv 7, 11 \mod 12$, then S is isogenous to the self-product of a supersingular elliptic curve over $\mathbf{F}_p$.

5. Congruence zeta function of the curve $y^2 = x(x^6 + a)$

PROPOSITION 5.1. *Let $\tilde{X}$ be the hyperelliptic curve over the finite field $\mathbf{F}_p$ defined by the affine equation $y^2 = x(x^6 + a)$. Put $\varepsilon = \pm 1$ and*

$$P(t) = (1-t)(1-pt)Z(\tilde{X}/\mathbf{F}_p, t)\,.$$

(1) *Suppose $p \equiv 1 \mod 12$. There exist uniquely pairs of integers (A, B) and (C, D) with*

$$A^2 + 3B^2 = p\,, \quad A \equiv 1 \mod 3\,, \quad B > 0$$

and

$$C^2 + D^2 = p\,, \quad C \equiv 1 \mod 4\,, \quad D > 0\,.$$

Put $\pi = A + B\sqrt{-3}$ and $\rho = C + D\sqrt{-1}$, and let χ denote the multiplicative character of $\mathbf{F}_p$ defined by $\alpha \mapsto \left(\frac{\alpha}{\pi,\rho}\right)_{12}$. Moreover put $\zeta = e^{\pi i/6}$.

Suppose $C \not\equiv 0 \mod 3$. Then we have:

(a) $P(t) = (1 - \varepsilon 2Ct + pt^2)^3$ *if* $\chi(a) = \varepsilon$;

(b) $P(t) = (1 - \varepsilon 2Dt + pt^2)^2(1 + \varepsilon 2Dt + pt^2)$ *if* $\chi(a) = \varepsilon\zeta^3$;

(c) $P(t) = (1 - \varepsilon 2Dt + (-C^2 + 3D^2)t^2 - \varepsilon 2Dpt^3 + p^2t^4)(1 - \varepsilon 2Dt + pt^2)$ *if* $\chi(a) = \varepsilon\zeta$;

(d) $P(t) = (1 + \varepsilon 2Ct + (3C^2 - D^2)t^2 + \varepsilon 2Cpt^3 + p^2t^4)(1 - \varepsilon 2Ct + pt^2)$ *if* $\chi(a) = \varepsilon\zeta^4$ *or* $-\varepsilon\zeta^2$;

(e) $P(t) = (1 - \varepsilon 2Dt + (-C^2 + 3D^2)t^2 - \varepsilon 2Dpt^3 + p^2t^4)(1 - \varepsilon 2Dt + pt^2)$ *if* $\chi(a) = \varepsilon\zeta^5$.

Suppose $C \equiv 0 \mod 3$. Then we have:

(a) $P(t) = (1 + \varepsilon 2Ct + pt^2)^2(1 - \varepsilon 2Ct + pt^2)$ *if* $\chi(a) = \varepsilon$;

(b) $P(t) = (1 + \varepsilon 2Dt + pt^2)^3$ *if* $\chi(a) = \varepsilon\zeta^3$;

(c) $P(t) = (1 + \varepsilon 2Dt + (-C^2 + 3D^2)t^2 + \varepsilon 2Dpt^3 + p^2t^4)(1 - \varepsilon 2Dt + pt^2)$ *if* $\chi(a) = \varepsilon\zeta$;

(d) *$P(t) = (1-\varepsilon 2Ct+(3C^2-D^2)t^2-\varepsilon 2Cpt^3+p^2t^4)(1-\varepsilon 2Ct+pt^2)$ if $\chi(a) = \varepsilon\zeta^4$ or $-\varepsilon\zeta^2$;*

(e) *$P(t) = (1 + \varepsilon 2Dt + (-C^2 + 3D^2)t^2 + \varepsilon 2Dpt^3 + p^2t^4)(1 - \varepsilon 2Dt + pt^2)$ if $\chi(a) = \varepsilon\zeta^5$.*

(2) *Suppose $p \equiv 5 \mod 12$. There exists uniquely a pair of integers (C, D) with*

$$C^2 + D^2 = p\,, \quad C \equiv 1 \mod 4\,, \quad D > 0\,.$$

Put $\rho = C + D\sqrt{-1}$, and let χ denote the multiplicative character of $\mathbf{F}_p$ defined by $\alpha \mapsto \left(\frac{\alpha}{\rho}\right)_4$. Then we have:

(a) *$P(t) = (1 + 2Dt + pt^2)(1 - 2Dt + pt^2)(1 - \varepsilon 2Ct + pt^2)$ if $\chi(a) = \varepsilon$;*

(b) *$P(t) = (1 + 2Ct + pt^2)(1 - 2Ct + pt^2)(1 - \varepsilon 2Dt + pt^2)$ if $\chi(a) = \varepsilon\sqrt{-1}$.*

(3) *Suppose $p \equiv 7 \mod 12$. There exists uniquely pair of integers (A, B) with*

$$A^2 + 3B^2 = p\,, \quad A \equiv 1 \mod 3\,, \quad A > 0\,.$$

Put $\rho = A+B\sqrt{-3}$, and let χ denote the multiplicative character of $\mathbf{F}_p$ defined by $\alpha \mapsto \left(\frac{\alpha}{\rho}\right)_3$. Then we have:

(a) *$P(t) = (1 + pt^2)^3$ if $\chi(a) = 1$;*

(b) *$P(t) = (1 + pt^2)(1 - pt^2 + p^2t^4)$ if $\chi(a) \neq 1$.*

(4) *Suppose $p \equiv 11 \mod 12$. Then we have $P(t) = (1 + pt^2)^3$.*

PROOF. Let Y and X be the hyperelliptic curves over the finite field $\mathbf{F}_p$ defined by $y^2 = x^{12} + a$ and by $y^2 = x^6 + a$, respectively, and let $J(Y)$, $J(X)$ and $J(\tilde{X})$ denote the Jacobian varieties of Y, X and $\tilde{X}$, respectively. We consider the covering $Y \to X$ defined by $(x, y) \mapsto (x^2, y)$ and the covering $Y \to \tilde{X}$ defined by $(x, y) \mapsto (x^2, xy)$. Then $J(Y)$ is isogenous to $J(X) \times J(\tilde{X})$ (cf. [7, Theorem C]). This implies that

$$P(J(Y)/\mathbf{F}_p; t) = P(J(X)/\mathbf{F}_p; t)P(J(\tilde{X})/\mathbf{F}_p; t)\,.$$

Therefore we can verify the assertion easily by Remark 1.10 and Theorem 4.2.

REMARK 5.2. [6] announced the assertions of Proposition 5.1 in a slightly different style.

REMARK 5.3. Let $\tilde{X}$ be the hyperelliptic curve over the finite field $\mathbf{F}_p$ defined by the affine equation $y^2 = x(x^6 + a)$.

If $p \equiv 1, 5 \mod 12$, then $J(\tilde{X})$ is isogenous the product of three ordinary elliptic curves with complex multiplication in $\mathbf{Q}(\sqrt{-1})$ over $\mathbf{F}_p$.

If $p \equiv 7, 11 \mod 12$, then $J(\tilde{X})$ is isogenous to the product of three supersingular elliptic curves over $\mathbf{F}_p$.

REMARK 5.4. It is known that if $p^i \equiv -1 \mod m$ for some integer $i > 0$, then the Fermat curve defined by $x^m + y^m = 1$ is supersingular, and therefore every curve which is a quotient of the Fermat curve is also supersingular (See [9]). This implies that the hyperelliptic curve defined by $y^2 = x^6+a$ over the finite field $\mathbf{F}_p$ is supersingular if $p \equiv 5 \mod 6$, and the hyperelliptic curves $y^2 = x^{12}+a$ and $y^2 = x(x^6+a)$ over the finite field $\mathbf{F}_p$ are supersingular if $p \equiv 11 \mod 12$. Therefore, from this fact, Prop 2.1 (2) and Theorem 3.1 (4), Theorem 4.1 (4), Proposition 5.1 (4) follow immediately.

References

[1] N. AOKI, Simple factors of the Jacobian of a Fermat curve and the Picard number of a product of Fermat curves, Amer. J. Math. **113** (1991), 779–833.

[2] B. C. BRENDT, R. J. EVANS and K. S. WILLIAMS, *Gauss and Jacobi sums*, Wiley-Interscience Publication, New York, 1998.

[3] J. BUHLER and N. KOBLITZ, Lattice basis reduction, Jacobi sums and hyperelliptic cryptosystems, Bull. Austral. Math. Soc. Vol. **58**(1998), 147–154.

[4] H. DAVENPORT and H. HASSE, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, J. Reine Angew. Math. **172** (1934), 151–182.

[5] E. FURUKAWA, M. KAWAZOE and T. TAKAHASHI, Counting points for hyperelliptic Curves of type $y^2 = x^5 + ax$ over finite prime fields, Selected Areas in *Cryptography* (SAC2003), Springer Verlag LNCS 3006, 2004, 24–41.

[6] M. HANEDA, M. KAWAZOE and T. TAKAHASHI, Formulae of the order of Jacobians for certain hyperelliptic curves, SCIS 2004, 885–890.

[7] E. KANI and M. ROSEN, Idempotent relations and factors of Jacobians, Math. Ann. **284** (1978), 307–327.

[8] E. OZAKI, Counting Points of the Curve $y^4 = x^3 + a$ over a Finite Field, Preprint (2006).

[9] T. SHIODA and T. KATSURA, On Fermat varieties, Tôhoku Math. J. **31** (1979), 97–115.

[10] A. WEIL, Jacobi sums as "Grössencharaktere", Trans. Amer. Math. Soc. **73** (1952), 487–495.

Present Address:
DEPARTMENT OF MATHEMATICS,
CHUO UNIVERSITY,
KASUGA, BUNKYO-KU, TOKYO, 112–8551 JAPAN.
e-mail: niitsuma@gug.math.chuo-u.ac.jp