JACOBSTHAL IDENTITY FOR $\mathbb{Q}(\sqrt{-2})$

KI-ICHIRO HASHIMOTO, LING LONG, AND YIFAN YANG

ABSTRACT. Let p be a prime congruent to 1 or 3 modulo 8 so that the equation $p = a^2 + 2b^2$ is solvable in integers. In this paper, we obtain closed-form expressions for a and b in terms of Jacobsthal sums. This is analogous to a classical identity of Jacobsthal.

1. INTRODUCTION

Let p be an odd prime. Recall that a famous result of Fermat states that p is the sum of two integer squares, i.e., $p = a^2 + b^2$ for some integers a and b, if and only if $p \equiv 1 \bmod 4$. It turns out there is a closed-form formula for the integers a and b in terms of the Legendre symbol $\left(\frac{\cdot}{p}\right)$. This is the classical identity of Jacobsthal.

Theorem A (Jacobsthal)**.** *Let p be a prime congruent to 1 modulo 4, and n be a quadratic nonresidue modulo p. Set*

$$A = \frac{1}{2}\sum_{x=0}^{p-1}\left(\frac{x^3 - x}{p}\right), \qquad B = \frac{1}{2}\sum_{x=0}^{p-1}\left(\frac{x^3 - nx}{p}\right). \tag{1}$$

Then $A, B \in \mathbb{Z}$ and $A^2 + B^2 = p$. More precisely, if, for a prime p congruent to 1 modulo 4, we let a be an odd integer and b be an even integer such that $p = a^2 + b^2$, then

$$\sum_{x=0}^{p-1}\left(\frac{x^3 - nx}{p}\right) = \begin{cases} \pm 2a, & \text{if } p \equiv 1 \bmod 4 \text{ and } \left(\frac{n}{p}\right) = 1, \\ \pm 2b, & \text{if } p \equiv 1 \bmod 4 \text{ and } \left(\frac{n}{p}\right) = -1, \\ 0, & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

In general, we shall refer to a sum of the form

$$\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right), \qquad f(x) \in \mathbb{Z}[x]$$

as a *Jacobsthal sum*.

There are many proofs for Jacobsthal's identity. Gauss supplied an elementary proof using only basic properties of the Legendre symbols. (See [2, Page 91].) One can also utilize properties of Jacobi sums to prove Theorem A. (See [1, Page 190].) On the other hand, the sums in (1) have the obvious meaning of counting points on the elliptic curves $y^2 = x^3 - x$ and $y^2 = x^3 - nx$ over $\mathbb{F}_p$, respectively, so it is possible to use tools from

Date: May 27, 2010.

2000 *Mathematics Subject Classification.* Primary 11L10; secondary 11G05, 11G15, 11G40.

Long was supported by NSA grant H98230-08-1-0076. Long and Yang would like to thank National Center for Theoretical Sciences in Hsinchu Taiwan at which place the project was initiated. Yang is supported by NSC Grant 97-2115-M-009-001. Part of this work was done while he visited the first author at the Waseda University. He would like to thank the first author and the Waseda University for the enormous hospitality.

arithmetic geometry to give yet another proof. In Section 2, we will briefly explain this approach.

Now observe that the equation $p = a^2 + b^2 = (a + bi)(a - bi)$ can be regarded as the prime factorization of p in the ring of integers $\mathbb{Z}[i]$ in the number field $\mathbb{Q}(i)$. Naturally, one may ask whether analogous identities exist in the case of other number fields. Let $\mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic number field with discriminant $-D$. If $\mathbb{Q}(\sqrt{-D})$ has class number one, then whether a prime p splits in $\mathbb{Q}(\sqrt{-D})$ depends solely on the value of $\left(\frac{-D}{p}\right)$. That is, if $\left(\frac{-D}{p}\right) = 1$, then there are integers a and b such that $p = f_D(a, b)$, where

$$f_D(x,y) = \begin{cases} x^2 + xy + \dfrac{1+D}{4}y^2, & \text{if } D \text{ is odd,} \\ x^2 + \dfrac{D}{4}y^2, & \text{if } D \text{ is even} \end{cases}$$

is the principal form of discriminant $-D$. Then one can ask whether these integers a and b can be expressed as Jacobsthal sums in a uniform way. For the case $D = 3$, it is relatively easy. Using Jacobi sums, we find the following analogue of Theorem A.

Theorem B (Chan-Long-Yang [3])**.** *Let p be a prime satisfying $p \equiv 1 \bmod 6$. Suppose n is any integer such that $x^3 \equiv n \bmod p$ is not solvable. Then*

$$3p = A^2 + AB + B^2,$$

where

$$A = \sum_{x=0}^{p-1} \left(\frac{x^3+1}{p}\right) \quad \text{and} \quad B = \left(\frac{n}{p}\right) \sum_{x=0}^{p-1} \left(\frac{x^3+n}{p}\right).$$

The main purpose of this paper is to prove an analogue of Jacobsthal's identity in the case $D = 8$. Note that $\left(\frac{-2}{p}\right) = 1$ if and only if $p \equiv 1, 3 \bmod 8$. For such a prime p, there exist integers a and b such that $p = a^2 + 2b^2$.

Theorem 1. *Let p be a prime congruent to 1 or 3 modulo 8. Let*

$$A = \frac{1}{2} \sum_{x=0}^{p-1} \left(\frac{x^3 + 4x^2 + 2x}{p}\right). \tag{2}$$

Moreover,

(1) *when $p \equiv 1 \bmod 8$ and n is a quadratic nonresidue modulo p, set*

$$B = \frac{1}{4} \sum_{x=0}^{p-1} \left(\frac{x^5 + nx}{p}\right), \tag{3}$$

and

(2) *when $p \equiv 3 \bmod 8$, set*

$$B = \frac{1}{4} \left(1 + \sum_{x=0}^{p-1} \left(\frac{x^6 + 4x^5 + 10x^4 - 20x^2 - 16x - 8}{p}\right)\right). \tag{4}$$

Then A and B are integers and satisfy $A^2 + 2B^2 = p$.

One remarkable feature of the main theorem is the existence of polynomials $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$ such that the integers A and B in $p = A^2+2B^2$ can be expressed as Jacobsthal sums associated to $f(x)$ and $g(x)$, respectively, for *all* primes p congruent to 3 modulo 8.

Our approach is mainly arithmetic-geometric. The elliptic curve $y^2 = x^3+4x^2+2x$ corresponding to the Jacobsthal sum in (2) has complex multiplication by the order $\mathbb{Z}[\sqrt{-2}]$. Thus, by a famous theorem of Deuring (see [7, Theorem II.10.5]), its L-function is the same as the L-function of a Hecke Grössencharakter on $\mathbb{Q}(\sqrt{-2})$. It is straightforward to verify that the quantity A in (2) has the same absolute value as the integer a in $p = a^2+2b^2$. The two hyperelliptic curves $y^2 = x^5 + nx$ and $y^2 = x^6 + 4x^5 + 10x^4 - 20x^2 - 16x - 8$ corresponding to the Jacobsthal sums in (3) and (4) are both isomorphic to $y^2 = x^5 + x$, although the two isomorphisms are over two different number fields. Thus, one can deduce information about the L-functions of the two hyperelliptic curves from that of $y^2 = x^5+x$. The details will be carried out in Section 3.

2. Arithmetic-geometric approach to Jacobsthal's identity

In this section, we will present an arithmetic-geometric proof of Theorem A. This will serve as an illustrating example how one can obtain information about the L-function of an algebraic curve over $\mathbb{Q}$ from that of another algebraic curve over $\mathbb{Q}$, assuming that the two curves are isomorphic over a number field.

For a nonzero integer n, let E_n denote the elliptic curve $y^2 = x^3 - nx$. Clearly, we have, for a prime p relatively prime to $2n$,

$$\#E_n(\mathbb{F}_p) = p + 1 + \sum_{x=0}^{p-1} \left(\frac{x^3 - nx}{p}\right).$$

Therefore, the reciprocal of the p-factor of $L(E_n/\mathbb{Q}, s)$ is equal to

$$1 + \left(\sum_{x=0}^{p-1} \left(\frac{x^3 - nx}{p}\right)\right) p^{-s} + p^{1-2s}.$$

For the case $n = 1$, the L-function $L(E_1/\mathbb{Q}, s)$ is well-known.

Lemma 1. *We have*

$$L(E_1/\mathbb{Q}, s) = \prod_{p\equiv 1 \bmod 4} \frac{1}{1 - 2\epsilon_p a_p p^{-s} + p^{1-2s}} \prod_{p\equiv 3 \bmod 4} \frac{1}{1 + p^{1-2s}},$$

where for $p \equiv 1 \bmod 4$*,* a_p *and* b_p *are positive integers with* a_p *odd and* b_p *even such that* $p = a_p^2 + b_p^2$*, and*

$$\epsilon_p = \left(\frac{-1}{a_p}\right)(-1)^{b_p/2}.$$

Proof. See [5, Page 59]. (Note that in [5], the L-function $L(E_1/\mathbb{Q}, s)$ is described differently, but it is easy to check that it gives the same L-function as above.) □

We now extract informations about $L(E_n/\mathbb{Q}, s)$ from the above lemma using the fact that E_1 and E_n are isomorphic over $\mathbb{Q}(\sqrt[4]{n})$.

Recall that for a given elliptic curve E defined over a number field K and an arbitrary rational prime ℓ, one can associate to E a continuous representation

$$\rho_{E,\ell} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(2, \mathbb{Q}_\ell)$$

via the Tate-module $T_\ell E$ of E. For detailed discussions, see [8]. In general, when C is a smooth irreducible curve defined over K of genus g, one can associate to C a $2g$-dimensional representation of $\mathrm{Gal}(\overline{K}/K)$ by considering the Tate module of the Jacobian of C. The L-function $L(\rho_{C,\ell}, s)$ of $\rho_{C,\ell}$ is defined by local Euler factors. Let $\mathcal{O}_K$ be the ring of integers of K. For any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ at which $\rho_{C,\ell}$ is unramified, the arithmetic Frobenius $\mathrm{Frob}_\mathfrak{p}$ acts on the representation space of $\rho_{C,\ell}$ with characteristic polynomial $P_\mathfrak{p}(T)$ of degree $2g$. Then the local Euler $\mathfrak{p}$-factor of $L(\rho_{C,\ell}, s)$ is $P_\mathfrak{p}(q^{-s})^{-1}$ where $q = |\mathcal{O}_K/\mathfrak{p}|$. Moreover, the Hasse-Weil zeta function of the reduction of C modulo $\mathfrak{p}$ is equal to

$$\frac{P_\mathfrak{p}(t)}{(1-t)(1-qt)}.$$

(cf. [6].) From now on, by the L-function $L(C, s)$ we mean the L-function $L(\rho_{C,\ell}, s)$ for any rational prime ℓ.

Now let us first recall a property of group representations.

Lemma 2. *Let G be a group and H be a normal subgroup of G of finite index such that G/H is cyclic. Assume that $\rho_1 : G \to \mathrm{GL}(V_1)$ and $\rho_2 : G \to \mathrm{GL}(V_2)$ are two irreducible representations over an algebraically closed field of characteristic not dividing $|G/H|$ such that the restrictions of ρ_1 and ρ_2 to H are isomorphic. Then $\rho_1 = \rho_2 \otimes \chi$ for some representation χ of G of degree 1 that is lifted from a character of G/H.*

Proof. See [4]. □

We now give a proof of Theorem A.

Proof of Theorem A. Let n be a nonsquare integer. Let E_1 and E_n denote the elliptic curves $y^2 = x^3 - x$ and $y^2 = x^3 - nx$. They are isomorphic over $\mathbb{Q}(\sqrt[4]{n})$, which is not Galois over $\mathbb{Q}$. Note that both curves have complex multiplication by the ring of Gaussian integers $\mathbb{Z}[i]$ as sending (x, y) to $(-x, iy)$ is an automorphism on both curves. Consequently,

$$\sum_{x=0}^{p-1} \left(\frac{x^3 - nx}{p}\right) = 0$$

when $p \equiv 3 \bmod 4$. For any rational prime ℓ, the Galois representations $\rho_{E_1,\ell}$ and $\rho_{E_n,\ell}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ are absolutely irreducible while their restrictions to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(i))$ decompose as

$$\rho_{E_1,\ell}\big|_{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(i))} = \pi_1 \oplus \bar{\pi}_1, \qquad \rho_{E_n,\ell}\big|_{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(i))} = \pi_n \oplus \bar{\pi}_n,$$

where π_1, π_n are 1-dimensional representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(i))$ and $\bar{\pi}_1, \bar{\pi}_n$ their complex conjugates respectively. Since E_1 and E_n are isomorphic over $L = \mathbb{Q}(i, \sqrt[4]{n})$,

$$\rho_{E_1,\ell}\big|_{\mathrm{Gal}(\overline{\mathbb{Q}}/L)} = \rho_{E_n,\ell}\big|_{\mathrm{Gal}(\overline{\mathbb{Q}}/L)}.$$

Without loss of generality we may assume that $\pi_1|_{\mathrm{Gal}(\overline{\mathbb{Q}}/L)} = \pi_n|_{\mathrm{Gal}(\overline{\mathbb{Q}}/L)}$. Then by Lemma 2, $\pi_1 = \pi_n \otimes \chi$ where χ is a character $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(i))$ lifted from a character of $\mathrm{Gal}(L/\mathbb{Q}(i)) \cong \mathbb{Z}/4\mathbb{Z}$ with kernel $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ as $L = \mathbb{Q}(i, \sqrt[4]{n})$ is the smallest field over which the two curves are isomorphic. When $p \equiv 1 \bmod 4$ and $p \nmid 2n\ell$, $\mathbb{F}_p(\sqrt[4]{n})$ is a quartic extension of $\mathbb{F}_p$ if and only if $\left(\frac{n}{p}\right) = -1$, i.e. $\chi(\mathrm{Frob}_p) = \pm i$ if and only if $\left(\frac{n}{p}\right) = -1$. By Lemma 1, $\mathrm{Re}\{\pi_1(\mathrm{Frob}_p)\} = \pm a$. Therefore, $\mathrm{Re}\{\pi_n(\mathrm{Frob}_p)\} = \mathrm{Re}\{\pi_1(\mathrm{Frob}_p) \otimes \chi(\mathrm{Frob}_p)\} = \pm a$ if $\left(\frac{n}{p}\right) = 1$ and $\mathrm{Re}\{\pi_n(\mathrm{Frob}_p)\} = \pm b$ otherwise. This proves the theorem. □

3. Proof of Theorem 1

In this section, we will prove Theorem 1. As explained in the introduction section, since the elliptic curve $y^2 = x^3 + 4x^2 + 2x$ has complex multiplication by $\mathbb{Z}[\sqrt{-2}]$, its L-function is easy to write down in terms of a Hecke Grössencharakter on $\mathbb{Q}(\sqrt{-2})$. This is done in Section 3.1. We then show that the hyperelliptic curve $y^2 = x^6 + 4x^5 + 10x^4 - 20x^2 - 16x - 8$ is isomorphic to $y^2 = x^5 + x$ over a Kummer extension L of $\mathbb{Q}(e^{2\pi i/8})$ and study the L-function of $y^2 = x^5 + x$ in Section 3.2. In Section 3.3, we will obtain the Hecke Grössencharakters associated to the cyclic extension $L/\mathbb{Q}(e^{2\pi i/8})$. Finally, we will give a proof of Theorem 1 in the last section.

3.1. The elliptic curve $y^2 = x^3 + 4x^2 + 2x$.

Lemma 3. *Let $E : y^2 = x^3 + 4x^2 + 2x$. The L-function $L(E/\mathbb{Q}, s)$ is given by*

$$\prod_{p\equiv 1,3 \bmod 8} \frac{1}{1 - 2\epsilon_p a_p p^{-s} + p^{1-2s}} \prod_{p\equiv 5,7 \bmod 8} \frac{1}{1 + p^{1-2s}},$$

where a_p and b_p are positive integers such that $p = a_p^2 + 2b_p^2$ and

$$\epsilon_p = \begin{cases} 2(-1)^{b_p/2}\left(\frac{-2}{a_p}\right), & \text{if } p \equiv 1 \bmod 8, \\ -2\left(\frac{-2}{a_p}\right), & \text{if } p \equiv 3 \bmod 8. \end{cases}$$

Proof. The elliptic curve $E : y^2 = x^3 + 4x^2 + 2x$ has complex multiplication by $\mathbb{Z}[\sqrt{-2}]$ and its conductor is 256. (See [7, Page 483].) Thus, by a well-known result of Deuring, the L-function $L(E/\mathbb{Q}, s)$ is identical with the L-function $L(\chi, s)$ of a Hecke Grössencharakter χ of the field $\mathbb{Q}(\sqrt{-2})$ of conductor $(\sqrt{-2})^5$. (See Theorem II.10.5 and Corollary II.10.5.1 of [7].) It is not difficult to work out this Hecke character. Namely, for each $a + b\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$, there are unique integers k, m, n with $0 \le k, m < 2$ and $0 \le n < 4$ such that

$$a + b\sqrt{-2} \equiv (-1)^k 3^m (1 + \sqrt{-2})^n \bmod (\sqrt{-2})^5.$$

Then the Hecke character χ is defined by

$$\chi(a + b\sqrt{-2}) = (-1)^{k+n}(a + b\sqrt{-2}).$$

(Note that since $\mathbb{Q}(\sqrt{-2})$ has class number one, we can define a Hecke character elementwise.) This character can be more succinctly written as

$$\chi(a + b\sqrt{-2}) = \left(\frac{-2}{a}\right)(a + b\sqrt{-2}) \cdot \begin{cases} (-1)^{b/2}, & \text{if } b \text{ is even}, \\ -1, & \text{if } b \text{ is odd}, \end{cases}$$

which yields the expression of $L(E/\mathbb{Q}, s)$ given in the statement of the lemma. □

Corollary 4. *We have*

$$\sum_{x=0}^{p-1} \left(\frac{x^3 + 4x^2 + 2x}{p}\right) = \begin{cases} \pm 2a, & \text{if } p \equiv 1, 3 \bmod 8, \\ 0, & \text{if } p \equiv 5, 7 \bmod 8, \end{cases}$$

where a and b are integers such that $p = a^2 + 2b^2$.

3.2. **The hyperelliptic curve** $y^2 = x^5 + x$.

Lemma 5. *The two hyperelliptic curves* $y^2 = x^5 + x$ *and* $y^2 = x^6 + 4x^5 + 10x^4 - 20x^2 - 16x - 8$ *are isomorphic over the number field* $\mathbb{Q}(\theta)$, *where* $\theta = 2^{3/4}(\sqrt{2} - 1)^{3/4}$.

Proof. Notice that the polynomial $x^6 + 4x^5 + 10x^4 - 20x^2 - 16x - 8$ factorizes as

$$(x^2 - 2)(x^4 + 4x^3 + 12x^2 + 8x + 4).$$

We make a linear transformation sending the root $\sqrt{2}$ to ∞ and the root $-\sqrt{2}$ to 0, i.e., setting

$$x = \frac{\sqrt{2}(x_1 + 1)}{x_1 - 1}, \qquad y = \frac{y_1}{(x_1 - 1)^3},$$

we get

$$y_1^2 = 128(2 + \sqrt{2})x_1(x_1^4 + 3 - 2\sqrt{2}).$$

Then let $x_1 = \sqrt{\sqrt{2} - 1}x_2$, $y_1 = y_2$, and obtain

$$y_2^2 = 128\sqrt{2}(\sqrt{2} - 1)^{3/2}(x_2^5 + x_2).$$

Finally, setting $x_2 = x_3$ and $y_2 = u^{1/2}y_3$, where $u = 128\sqrt{2}(\sqrt{2} - 1)^{3/2}$, we arrive at

$$y_3^2 = x_3^5 + x_3.$$

This proves the lemma. □

Proposition 6. *Let* X *be the hyperelliptic curve* $y^2 = x^5 + x$ *over* $\mathbb{Q}$. *Then we have*

$$L(X/\mathbb{Q}, s) = L(E_1/\mathbb{Q}, s)L(E_2/\mathbb{Q}, s),$$

where E_1 *and* E_2 *are the elliptic curves* $y^2 = x^3 + 4x^2 + 2x$ *and* $y^2 = x^3 - 4x^2 + 2x$, *respectively.*

Proof. We have

$$x^5 + x = x((x - 1)^4 + 4x(x - 1)^2 + 2x^2).$$

Thus, letting

$$X = \frac{(x - 1)^2}{x}, \qquad Y = \frac{y(x - 1)}{x^2},$$

we find that X and Y satisfy $Y^2 = X^3 + 4X^2 + 2X$. In other words, there is a 2-to-1 morphism from X to E_1 defined over $\mathbb{Q}$ and hence the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-representation $\rho_{E_1,\ell}$ associated to E_1 is a subrepresentation of $\rho_{X,\ell}$ associated to X. Similarly, setting $X = (x+1)^2/x$ and $Y = y(x+1)/x^2$, we get a morphism from X to E_2 and conclude that $\rho_{E_1,\ell}$ is also a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-subrepresentation of $\rho_{X,\ell}$. Since $\rho_{E_1,\ell}$ and $\rho_{E_2,\ell}$ are nonisomorphic absolutely irreducible $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-representations and $\dim_{\mathbb{Q}_\ell} \rho_{E_1,\ell} + \dim_{\mathbb{Q}_\ell} \rho_{E_2,\ell} = \dim_{\mathbb{Q}_\ell} \rho_{X,\ell}$, we have

$$\rho_{X,\ell} = \rho_{E_1,\ell} \oplus \rho_{E_2,\ell}$$

and

$$L(X/\mathbb{Q}, s) = L(E_1/\mathbb{Q}, s)L(E_2/\mathbb{Q}, s).$$

This proves the proposition. □

Corollary 7. *Let the curve* $X : y^2 = x^5 + x$ *be given as above. Let*

$$\frac{1}{(1 - \alpha_{p,1}p^{-s}) \dots (1 - \alpha_{p,4}p^{-s})}$$

be the p*-factor of* $L(X/\mathbb{Q}, s)$.

(1) *If* $p \equiv 1 \bmod 8$*, then*

$$\alpha_{p,j} = \left(\frac{-2}{a}\right)(-1)^{b/2}(a \pm b\sqrt{-2}),$$

each with multiplicity 2*, where* a *and* b *are the positive integers such that* $p = a^2 + 2b^2$.

(2) *If* $p \equiv 3 \bmod 8$*, then* $\alpha_{p,j} = \pm a \pm b\sqrt{-2}$*, where* a *and* b *are integers such that* $p = a^2 + 2b^2$.

(3) *If* $p \equiv 5, 7 \bmod 8$*, then* $\alpha_{p,j} = \pm i\sqrt{p}$*, each with multiplicity* 2.

Proof. This corollary follows immediately from Proposition 6, Lemma 3, and the fact that $y^2 = x^3 - 4x^2 + 2x$ is a quadratic twist of $y^2 = x^3 + 4x^2 + 2x$ by -1, i.e. it is isomorphic to $-y^2 = x^3 + 4x^2 + 2x$ over $\mathbb{Q}(i)$. □

3.3. **The number field** $\mathbb{Q}(\theta, i)$**.** Let $\theta = 2^{3/4}(\sqrt{2}-1)^{3/4}$. In the previous section, we have seen that the two hyperelliptic curves $y^2 = x^5 + x$ and $y^2 = x^6 + 4x^5 + 10x^4 - 20x^2 - 16x - 8$ are isomorphic over $\mathbb{Q}(\theta)$. As in the case of Theorem A, the field $\mathbb{Q}(\theta)$ is not an abelian extension of $\mathbb{Q}$, so in order to apply Lemma 2, we change the base field from $\mathbb{Q}$ to $\mathbb{Q}(\zeta_8)$, where $\zeta_8 = e^{2\pi i/8}$ so that $\mathbb{Q}(\theta, \zeta_8)$ is Galois over $\mathbb{Q}(\zeta_8)$. From now on, we let

$$K = \mathbb{Q}(\zeta_8), \qquad L = \mathbb{Q}(\theta, \zeta_8) = \mathbb{Q}(\theta, i).$$

Lemma 8. *The field* $L = \mathbb{Q}(\theta, i)$ *is a Kummer extension of* $K = \mathbb{Q}(\zeta_8)$ *obtained by adjoining the fourth root of* $i(\sqrt{2}-1)$ *to* $\mathbb{Q}(\zeta_8)$*. The field extension* L/K *is unramified outside of the place* $1 - \zeta_8$.

Proof. We have $(1-\zeta_8)^4 = 2(\sqrt{2}-1)^2 i$. Thus, $(\theta/(1-\zeta_8)^3)^4 = ((\sqrt{2}-1)i)^{-3}$ and $\mathbb{Q}(\theta, i) = \mathbb{Q}(\sqrt[4]{i(\sqrt{2}-1)}, \zeta_8)$. Now $i(\sqrt{2}-1)$ is a unit in $\mathbb{Z}[\zeta_8]$. Hence, the only place at which L/K can possibly be ramified is the prime $1 - \zeta_8$ lying over 2. This proves the lemma. □

The main purpose of this section is to determine the characters of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ associated to the abelian extension L/K. From now on, we set

$$\eta = \sqrt[4]{i(\sqrt{2}-1)}.$$

(Since L/K is a Kummer extension, it does not matter which fourth root of $i(\sqrt{2}-1)$ we take.) The Galois group of L over K is cyclic and generated by

$$\sigma : \eta \mapsto i\eta.$$

For each prime ideal $\mathfrak{p}$ of $\mathbb{Q}(\zeta_8)$ relatively prime to $1 - \zeta_8$, the Artin symbol $\left(\frac{L/K}{\mathfrak{p}}\right)$ is defined as the unique Galois element σ^j such that

$$\sigma^j(\eta) \equiv \eta^{Nm(\mathfrak{p})} \bmod \mathfrak{p}, \tag{5}$$

where $Nm(\mathfrak{p})$ denotes the norm of $\mathfrak{p}$. Then the characters associated to the field extension L/K are defined by

$$\chi_k(\mathfrak{p}) = i^{jk}, \qquad k = 0, \ldots, 3, \tag{6}$$

where j is the integer in (5).

Lemma 9. *Let* $k = 1, 2, 3$.

(1) *If $\mathfrak{p}$ is a prime of $\mathbb{Q}(\zeta_8)$ lying over a prime p congruent to 3 modulo 8, then $\chi_k(\mathfrak{p}) = i^k$ or i^{-k}.*
(2) *If $\mathfrak{p}$ is a prime of $\mathbb{Q}(\zeta_8)$ lying over a prime p congruent to 5 or 7 modulo 8, then $\chi_k(\mathfrak{p}) = 1$ for all k.*

Proof. A prime $\mathfrak{p}$ lying over a prime p congruent to 3, 5, or 7 modulo 8 has norm p^2. In the case $p \equiv 3 \bmod 8$, notice that

$$(\sqrt{2}-1)^{p+1} \equiv (-\sqrt{2}-1)(\sqrt{2}-1) = -1 \bmod p,$$

which implies that

$$(\sqrt{2}-1)^{(p^2-1)/2} \equiv -1 \bmod p.$$

It follows that

$$\eta^{Nm(\mathfrak{p})-1} = (i(\sqrt{2}-1))^{(p^2-1)/4} \equiv \pm i \bmod \mathfrak{p},$$

and $\chi_k(\mathfrak{p}) = \pm i^k$.

If $p \equiv 5 \bmod 8$, a similar argument shows that

$$(\sqrt{2}-1)^{(p^2-1)/4} = \left((\sqrt{2}-1)^{p+1}\right)^{(p-1)/4} \equiv (-1)^{(p-1)/4} = -1 \bmod \mathfrak{p}$$

and

$$\eta^{Nm(\mathfrak{p})-1} = (i(\sqrt{2}-1))^{(p^2-1)/4} \equiv 1 \bmod \mathfrak{p},$$

which implies $\chi_k(\mathfrak{p}) = 1$ for all $k = 0, \ldots, 3$.

If $p \equiv 7 \bmod 8$, we have $\sqrt{2} \equiv u \bmod p$ for some $u \in \mathbb{Z}$. Then

$$(\sqrt{2}-1)^{(p^2-1)/4} \equiv \left((u-1)^{p-1}\right)^{(p+1)/4} \equiv 1 \bmod \mathfrak{p}$$

and

$$\eta^{Nm(\mathfrak{p})-1} = (i(\sqrt{2}-1))^{(p^2-1)/4} \equiv 1 \bmod \mathfrak{p}.$$

Again, this gives us $\chi_k(\mathfrak{p}) = 1$ for all k. This proves the lemma. □

3.4. **Proof of Theorem 1.** We now prove Theorem 1. As before, we let

$$K = \mathbb{Q}(\zeta_8), \qquad L = \mathbb{Q}(\theta, \zeta_8),$$

where $\theta = 2^{3/4}(\sqrt{2}-1)^{3/4}$. For a given number field F, denote $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ by G_F for convenience.

The cases $p \equiv 1 \bmod 8$ can be proved in a similar way as Theorem A. For instance, one can utilize Theorem 6.2.3 of [1] to conclude that

$$\sum_{x=0}^{p-1} \left(\frac{x^5+nx}{p}\right) = \pm 4b,$$

provided that p is a prime congruent to 1 modulo 8, n is a quadratic nonresidue modulo p, and a and b are integers such that $p = a^2 + 2b^2$. Then from Corollary 4, we get the claimed identity. Alternatively, one can also follow the argument in Section 2 to get the same conclusion. We shall not give details here.

Now consider the two hyperelliptic curves $X_1 : y^2 = x^5 + x$ and $X_2 : y^2 = x^6 + 4x^5 + 10x^4 - 20x^2 - 16x - 8$. Assume that the p-factors of the L-functions of $X_1/\mathbb{Q}$ and $X_2/\mathbb{Q}$ are

$$\frac{1}{(1-\alpha_{p,1}p^{-s})\ldots(1-\alpha_{p,4}p^{-s})}, \qquad \frac{1}{(1-\beta_{p,1}p^{-s})\ldots(1-\beta_{p,4}p^{-s})},$$

respectively. Then for $p \not\equiv 1 \bmod 8$, the p-factors of the L-functions of X_1/K and X_2/K are

$$\frac{1}{(1-\alpha_{p,1}^2 p^{-2s})^2 \dots (1-\alpha_{p,4}^2 p^{-2s})^2}, \qquad \frac{1}{(1-\beta_{p,1}^2 p^{-2s})^2 \dots (1-\beta_{p,4}^2 p^{-2s})^2},$$

respectively.

Counting the numbers of points on $X_2(\mathbb{F}_{3^n})$, we find that the 3-factor of $L(X_2/\mathbb{Q}, s)$ is

$$(1 + 4 \cdot 3^{-s} + 8 \cdot 3^{-2s} + 12 \cdot 3^{-3s} + 9 \cdot 3^{-4s})^{-1},$$

which implies that

$$\beta_{3,j} = \zeta_8(1+\sqrt{-2}),\ \zeta_8^3(1+\sqrt{-2}),\ \zeta_8^5(1-\sqrt{-2}),\ \zeta_8^7(1-\sqrt{-2}),$$

and

$$\beta_{3,j}^2 = \pm i(1+\sqrt{-2})^2,\ \pm i(1-\sqrt{-2})^2. \tag{7}$$

On the other hand, from Corollary 7, we know that

$$\alpha_{3,j}^2 = (1 \pm \sqrt{-2})^2, \tag{8}$$

each with multiplicity 2.

From the above data, we proceed to determine the structure of the semisimplification of $\rho_{X_2,\ell}|_{G_K}$ from $\rho_{X_1,\ell}|_{G_K}$ and consider them as representations over $\overline{\mathbb{Q}}_\ell$. By the discussion in Section 3.2, we know $\rho_{X_1,\ell} = \rho_{E_1,\ell} \oplus \rho_{E_2,\ell}$ where $\rho_{E_1,\ell}|_{G_K} \cong \rho_{E_2,\ell}|_{G_K}$. As $\sqrt{-2} \in K$, $\rho_{E_1,\ell}|_{G_K} = \sigma \oplus \bar{\sigma}$ for some one-dimensional representation σ of G_K and its complex conjugate. Moreover, the restriction $\sigma|_{G_L}$ of σ to G_L is not isomorphic to $\bar{\sigma}|_{G_L}$. Since $\rho_{X_1,\ell}|_{G_L} \cong \rho_{X_2,\ell}|_{G_L}$, we know

$$\rho_{X_2,\ell}|_{G_L} = \sigma|_{G_L} \oplus \sigma|_{G_L} \oplus \bar{\sigma}|_{G_L} \oplus \bar{\sigma}|_{G_L}.$$

Let $(\rho_{X_1,\ell}|_{G_K})^{ss}$ be the semisimplification of $\rho_{X_1,\ell}|_{G_K}$. Since $\mathrm{Gal}(L/K) \cong \mathbb{Z}/4\mathbb{Z}$, by Lemma 2, each G_K irreducible component of $(\rho_{X_1,\ell}|_{G_K})^{ss}$ is either isomorphic to σ or $\bar{\sigma}$ up to at most a character of G_K whose kernel contains G_L. Thus we may write

$$(\rho_{X_1,\ell}|_{G_K})^{ss} = (\sigma \otimes \phi_1) \oplus (\sigma \otimes \phi_2) \oplus (\bar{\sigma} \otimes \phi_3) \oplus (\bar{\sigma} \otimes \phi_4),$$

for some characters ϕ_i of G_K. Combined with the above data at $p = 3$, we conclude that ϕ_i has order 4, $\phi_3 = \phi_1$, and $\phi_2 = \phi_4$. Without loss of generality we may assume

$$\phi = \chi_1, \quad \phi^{-1} = \chi_3, \tag{9}$$

where χ_1, χ_3 are defined in (6). In summary

$$(\rho_{X_1,\ell}|_{G_K})^{ss} = (\sigma \otimes \chi_1) \oplus (\sigma \otimes \chi_3) \oplus (\bar{\sigma} \otimes \chi_1) \oplus (\bar{\sigma} \otimes \chi_3).$$

Now we turn our attention to general primes p that are congruent to 3 modulo 8. For such a prime p, we have $p = a_p^2 + 2b_p^2$ for some integers a_p and b_p. From Corollary 7, we know that

$$\alpha_{p,j}^2 = (a_p \pm b_p\sqrt{-2})^2,$$

each with multiplicity 2. Then by Lemma 9, regardless of which $\mathfrak{p}$ lying over p, we have $\chi_k(\mathfrak{p}) = \pm i$. Thus, β_{p,k_p}^2 is equal to one of the numbers

$$\pm i(a_p \pm b_p\sqrt{-2})^2,$$

and consequently, β_{p,k_p} is one of

$$\zeta_8^m(a_p \pm b_p\sqrt{-2}), \quad m = 1, 3, 5, 7.$$

Because $\beta_{p,k}$, $k = 1, \ldots, 4$, are Galois conjugates over $\mathbb{Q}$, we conclude that the p-factor of $L(X_2/\mathbb{Q}, s)$ is equal to one of

$$\frac{1}{1 \pm 4b_p p^{-s} + 8b_p^2 p^{-2s} \pm 4b_p p^{1-3s} + p^{2-4s}}.$$

In other words, we have

$$\#X_2(\mathbb{F}_p) = p + 1 \pm 4b_p.$$

On the other hand, because the polynomial $x^6 + 4x^5 + 10x^4 - 20x^2 - 16x - 8$ has an even degree and its leading coefficient is a square, we have

$$\#X_2(\mathbb{F}_p) = p + 2 + \sum_{x=0}^{p-1} \left(\frac{x^6 + 4x^5 + 10x^4 - 20x^2 - 16x - 8}{p} \right).$$

Therefore,

$$1 + \sum_{x=0}^{p-1} \left(\frac{x^6 + 4x^5 + 10x^4 - 20x^2 - 16x - 8}{p} \right) = \pm 4b_p.$$

Together with Lemma 3, this yields our main theorem.

REFERENCES

[1] Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams. *Gauss and Jacobi sums*. Canadian Mathematical Society Series of Monographs and Advanced Texts. John Wiley & Sons Inc., New York, 1998. A Wiley-Interscience Publication.

[2] Jan Hendrik Bruinier, Gerard van der Geer, Günter Harder, and Don Zagier. *The 1-2-3 of modular forms*. Universitext. Springer-Verlag, Berlin, 2008. Lectures from the Summer School on Modular Forms and their Applications held in Nordfjordeid, June 2004, Edited by Kristian Ranestad.

[3] Heng Huat Chan, Ling Long, and Yifan Yang. A cubic analogue of the Jacobsthal identity. *Amer. Math. Monthly*, to appear.

[4] A. H. Clifford. Representations induced in an invariant subgroup. *Ann. of Math. (2)*, 38(3):533–550, 1937.

[5] Neal Koblitz. *Introduction to elliptic curves and modular forms*, volume 97 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1993.

[6] James S. Milne. Abelian varieties (v2.00), 2008. Available at www.jmilne.org/math/.

[7] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[8] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

DEPARTMENT OF MATHEMATICS, WASEDA UNIVERSITY, 3-4-1, OKUBO SHINJUKU-KU, TOKYO 169, JAPAN

E-mail address: `khasimot@waseda.ac.jp`

DEPARTMENT OF MATHEMATICS, IOWA STATE UNIVERSITY, AMES, IA 50011, USA

E-mail address: `linglong@iastaate.edu`

DEPARTMENT OF APPLIED MATHEMATICS, NATIONAL CHIAO TUNG UNIVERSITY AND NATIONAL CENTER FOR THEORETICAL SCIENCES, HSINCHU, TAIWAN

E-mail address: `yfyang@math.nctu.edu.tw`