

A Quadratic Curve Analogue of the Taniyama-Shimura Conjecture

Masahito Hayashi¹, Kazuyasu Shigemoto^{2,*}, and Takuya Tsukioka³


ABSTRACT

For quadratic curves over finite fields, the number of solutions, which is governed by an analogue of the Mordell-Weil group, is expressed with the Legendre symbol of a coefficient of quadratic curves. Focusing on the number of solutions, a quadratic curve analogue of the modular form in the Taniyama-Shimura conjecture is proposed. This modular form yields the Gaussian sum and also possesses some modular transformation structure.

Keywords: Analogue of the modular form, analogue of the Taniyama-Shimura conjecture, generalized Gaussian sum.

Submitted: September 24, 2024

Published: November 13, 2024

 10.24018/ejmath.2024.5.6.378

¹Osaka Institute of Technology, Japan.

²Tezukayama University, Japan.

³Bukkyo University, Japan.

*Corresponding Author:

e-mail: shigemot@tezukayama-u.ac.jp

1. INTRODUCTION

For exactly solvable models in non-linear systems, the group structure plays an important role. The KdV equation is one of the examples. The AKNS formalism exposes that the KdV equation has the $sl(2, \mathbf{R}) \cong so(2, 1)/\mathbf{Z}_2 \cong sp(2, \mathbf{R}) \cong su(1, 1)$ Lie algebra structure [1]. From geometrical approaches, we can also observe that the KdV equation has such Lie algebra structure [2]–[5]. In addition, we can find the Lie group structure for the Jacobi type elliptic function [6]. It is worth mentioning that the \wp -function is one of the static solutions of the KdV equation. While, in some sense, the Taniyama-Shimura conjecture [7]–[9] is considered to be the exactly solvable system because we can obtain all solutions for each elliptic curve over specific \mathbf{F}_p from the Mordell-Weil group structure [10], [11] of that elliptic curve. Parametrizing elliptic curves by the \wp -function, the Lie group structure of the \wp -function and the Mordell-Weil group in the Taniyama-Shimura conjecture are strongly connected. The Mordell-Weil group can be considered to be the special Abelian subgroup of the non-Abelian $SL(2, \mathbf{R})$ Lie group. In the Taniyama-Shimura conjecture, the Mordell-Weil group plays an essential role.

In this paper, we consider an analogue of the Taniyama-Shimura conjecture for quadratic curves over \mathbf{F}_p . By constructing the analogue of the modular form of the Taniyama-Shimura conjecture for quadratic curves, we will demonstrate that such an analogue of the modular form can be considered as a generalization of the Gaussian sum and it has a structure of the modular transformation by using the other Gaussian sum.

2. GENERALIZED GAUSSIAN SUM

Here we consider the quadratic curve analogue of the modular form of the Taniyama-Shimura conjecture.

2.1. The Quadratic Curve Analogue of the Modular Form of the Taniyama-Shimura Conjecture

We denote the number of solutions for the elliptic curve

$$y^2 \equiv x^3 + k_2x^2 + k_1x + k_0 \pmod{p},$$



over \mathbf{F}_p by $\widehat{N}(p)$ and define $\widehat{b}(p) = p - \widehat{N}(p)$. Suppose a modular form, which corresponds to this elliptic curve, to be

$$f(\tau) = \sum_{n=1}^{\infty} \widehat{c}(n)q^n, \quad q = \exp(2\pi i\tau).$$

Then the Taniyama-Shimura conjecture claims $\widehat{b}(p) = \widehat{c}(p)$ for prime numbers p . In our quadratic case, i.e.,

$$y^2 \equiv ax^2 + 1 \pmod{p},$$

over \mathbf{F}_p , the number of solutions is given by $N(p) = p - \left(\frac{a}{p}\right)$ and we define $b(p) = p - N(p) = \left(\frac{a}{p}\right)$. Then the quadratic curve analogue of the modular form is given by

$$f(\tau) = \sum_{n=1}^{\infty} c(n)q^n, \quad q = \exp(2\pi i\tau).$$

with $c(p) = b(p) = \left(\frac{a}{p}\right)$ for prime numbers p .

Based on the above discussions, the quadratic curve analogue of the modular form should at least include $\left(\frac{a}{p}\right)q^p$ terms. For such a form to have some modular transformation property, it must include terms $b(n)q^n$ with a non-prime integer n . Candidate that satisfies these requirements can be obtained by replacing the prime number p with any integer n . At the same time, we have to replace the Legendre symbol with the Kronecker symbol in the form $\left(\frac{a}{p}\right)q^p \rightarrow \left(\frac{a}{n}\right)_K q^n$, because the Legendre symbol is not defined for non-prime integer n . Note that for odd prime number p , $\left(\frac{a}{p}\right)_K = \left(\frac{a}{p}\right)$.

Let us discuss the periodicities of the Kronecker symbol. For $a \equiv 1 \pmod{4}$, we obtain

$$\left(\frac{a}{p}\right)_K = \left(\frac{p}{a}\right)_K (-1)^{\frac{a-1}{2} \cdot \frac{p-1}{2}} = \left(\frac{p+a\ell}{a}\right)_K (-1)^{\frac{a-1}{2} \cdot \frac{p+a\ell-1}{2}} = \left(\frac{a}{p+a\ell}\right)_K,$$

for any integer ℓ . That is, $\left(\frac{a}{p}\right)_K$ is periodic with respect to $p \pmod{a}$.

For $a \equiv 3 \pmod{4}$, we obtain

$$\left(\frac{a}{p}\right)_K = \left(\frac{p}{a}\right)_K (-1)^{\frac{a-1}{2} \cdot \frac{p-1}{2}} = \left(\frac{p+4a\ell}{a}\right)_K (-1)^{\frac{a-1}{2} \cdot \frac{p+4a\ell-1}{2}} = \left(\frac{a}{p+4a\ell}\right)_K.$$

That is, $\left(\frac{a}{p}\right)_K$ is periodic with respect to $p \pmod{4a}$.

For $a \equiv 2 \pmod{4}$, we put $a = 2a'$ with a' is odd integer. Then we have

$$\begin{aligned} \left(\frac{a}{p}\right)_K &= \left(\frac{2}{p}\right)_K \left(\frac{a'}{p}\right)_K = (-1)^{\frac{p^2-1}{8}} \left(\frac{p}{a'}\right)_K (-1)^{\frac{a'-1}{2} \cdot \frac{p-1}{2}} \\ &= (-1)^{\frac{(p+8a'\ell)^2-1}{8}} \left(\frac{p+8a'\ell}{a'}\right)_K (-1)^{\frac{a'-1}{2} \cdot \frac{p+8a'\ell-1}{2}} = \left(\frac{a}{p+4a\ell}\right)_K. \end{aligned}$$

That is, $\left(\frac{a}{p}\right)_K$ is periodic with respect to $p \pmod{4a}$.

Then we arrive at the quadratic curve analogue of the modular form

$$f(\tau) = \begin{cases} \sum_{n=1}^{\infty} \left(\frac{a}{n}\right)_K q^n, & q = \exp(2\pi i\tau), \quad \text{if } a \equiv 1 \pmod{4}, \\ \sum_{\substack{n=1 \\ (n,4a)=1}}^{\infty} \left(\frac{a}{n}\right)_K q_1^n, & q_1 = \exp(2\pi i\tau/4), \quad \text{if } a \equiv 2, 3 \pmod{4}. \end{cases} \quad (1)$$

In order to concrete our claim, we will show the following in subsequent subsections:

- 1) $f(\tau)$ becomes the Gaussian sum if τ is the special value τ_0 ,
- 2) $f(\tau)$ is associated with the theta function, so it has the structure of the modular transformation.

Then we call the above infinite sum (1) the generalized Gaussian sum. If τ is the special value τ_0 , the generalized Gaussian sum becomes periodic, and we denote one of its periods, which is proportional to the Gaussian sum, as $\bar{f}(\tau_0)$.

We close this subsection by giving some examples of $\bar{f}(\tau_0)$, which will be helpful to understand the proof in the following subsections.

Example 1.

- 1) For $y^2 \equiv 5x^2 + 1 \pmod{p}$, $\bar{f}(1/5) = q - q^2 - q^3 + q^4 = \sqrt{5} = G_5$.
- 2) For $y^2 \equiv -3x^2 + 1 \pmod{p}$, $\bar{f}(1/3) = q - q^2 = \sqrt{-3} = G_3$.
- 3) For $y^2 \equiv 3x^2 + 1 \pmod{p}$, $\bar{f}(1/3) = q_1 - q_1^5 = \sqrt{3} = -iG_3$.
- 4) For $y^2 \equiv -5x^2 + 1 \pmod{p}$, $\bar{f}(1/5) = q_1 + q_1^3 + q_1^7 + q_1^9 = \sqrt{-5} = iG_5$

2.2. Gaussian Sum

In this subsection, we show that the Gaussian sum can be extracted from the quadratic curve analogue of the modular form given in (1).

Here we list the properties of the Kronecker symbol used in the following calculations. Let $m = 2^{e_1}m'$, $n = 2^{e_2}n'$ ($m', n' = \text{odd integer}$):

•

if $m > 0$ or $n > 0$ and $(m, n) = 1$ ($e_1 = 0$ or $e_2 = 0$ and $(m', n') = 1$),

$$\left(\frac{n}{m}\right)_K \left(\frac{m}{n}\right)_K = (-1)^{\frac{m'-1}{2} \cdot \frac{n'-1}{2}}. \quad (2)$$

•

$$\left(\frac{n}{2}\right)_K = \left(\frac{2}{n}\right)_K = \begin{cases} 1, & \text{if } n \equiv 1, 7 \pmod{8}, \\ -1, & \text{if } n \equiv 3, 5 \pmod{8}, \\ 0, & \text{if } 2|n. \end{cases} \quad (3)$$

•

$$\left(\frac{-1}{n}\right)_K = (-1)^{\frac{n'-1}{2}}. \quad (4)$$

•

if $n \neq -1$,

$$\left(\frac{ab}{n}\right)_K = \left(\frac{a}{n}\right)_K \left(\frac{b}{n}\right)_K, \quad \left(\frac{n}{ab}\right)_K = \left(\frac{n}{a}\right)_K \left(\frac{n}{b}\right)_K. \quad (5)$$

•

$$\left(\frac{m}{n}\right)_K = \pm 1, \text{ if } (m, n) = 1, \text{ otherwise } \left(\frac{m}{n}\right)_K = 0. \quad (6)$$

•

$$\text{for } n > 0 \text{ and } a \equiv b \pmod{n} \begin{cases} 4n, & \text{if } n \equiv 2 \pmod{4}, \\ n, & \text{otherwise,} \end{cases}, \quad \left(\frac{a}{n}\right)_K = \left(\frac{b}{n}\right)_K. \quad (7)$$

1) $y^2 \equiv ax^2 + 1 \pmod{p}$, $a > 0$ and $a \equiv 1 \pmod{4}$: In the case of $(n, a) = 1$, $\left(\frac{a}{n}\right)_K = \left(\frac{n}{a}\right)_K$ is derived from (2). Since $\left(\frac{a}{n}\right)_K = 0$ if $(n, a) \neq 1$, (1) can be rewritten as

$$f(\tau) = \sum_{n=1}^{\infty} \left(\frac{n}{a}\right)_K q^n, \quad q = \exp(2\pi i\tau). \quad (8)$$

Equation (7) shows that $\left(\frac{n+a}{a}\right)_K = \left(\frac{n}{a}\right)_K$ holds. If $\tau = 1/a$, then $q^a = 1$, and we obtain

$$\left(\frac{n+a}{a}\right)_K q^{n+a} = \left(\frac{n}{a}\right)_K q^n.$$

From this equation, it can be seen that $f(1/a)$ repeatedly contains $\bar{f}(1/a)$ shown in the following

$$\bar{f}(1/a) = \sum_{n=1}^{a-1} \left(\frac{n}{a}\right)_K \exp(2\pi in/a). \quad (9)$$

Since $\left(\frac{a}{a}\right)_K = 0$, the sum of n in (9) is up to $a - 1$.

If we put $a = p$ (prime number) further, $\bar{f}(1/p)$ becomes the Gaussian sum in the form

$$\bar{f}(1/p) = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \exp(2\pi in/p) = G_p = \sqrt{p}, \quad p \equiv 1 \pmod{4}. \quad (10)$$

2) $y^2 \equiv ax^2 + 1 \pmod{p}$, $a < 0$ and $a \equiv 1 \pmod{4}$: Let us consider for $a \equiv 1 \pmod{4}$ and $a < 0$. In this case we rewrite $\left(\frac{a}{n}\right)_K$ as

$$\left(\frac{a}{n}\right)_K = \left(\frac{-|a|}{n}\right)_K = \left(\frac{-1}{n}\right)_K \left(\frac{|a|}{n}\right)_K = (-1)^{\frac{n'-1}{2}} \times (-1)^{\frac{|a|-1}{2} \cdot \frac{n'-1}{2}} \left(\frac{n}{|a|}\right)_K$$

by using (2), (4) and (5). Note that $(-1)^{\frac{|a|-1}{2}} = -1$ because of $|a| \equiv 3 \pmod{4}$. Then we obtain

$$(-1)^{\frac{n'-1}{2}} \times (-1)^{\frac{|a|-1}{2} \cdot \frac{n'-1}{2}} = (-1)^{\frac{n'-1}{2}} \times (-1)^{\frac{n'-1}{2}} = 1.$$

Then (1) can be rewritten as

$$f(\tau) = \sum_{n=1}^{\infty} \left(\frac{n}{|a|}\right)_K q^n, \quad q = \exp(2\pi i\tau). \quad (11)$$

If $\tau = 1/|a|$, then $q^{|a|} = 1$, and we obtain

$$\left(\frac{n+|a|}{|a|}\right)_K q^{n+|a|} = \left(\frac{n}{|a|}\right)_K q^n.$$

The generalized Gaussian sum $f(1/|a|)$ repeatedly contains $\bar{f}(1/|a|)$ shown in the following

$$\bar{f}(1/|a|) = \sum_{n=1}^{|a|-1} \left(\frac{n}{|a|}\right)_K \exp(2\pi in/|a|). \quad (12)$$

If we put $|a| = p$ (prime number) further, $\bar{f}(1/p)$ becomes the Gaussian sum in the form

$$\bar{f}(1/p) = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \exp(2\pi in/p) = G_p = i\sqrt{p}, \quad p \equiv 3 \pmod{4}. \quad (13)$$

3) $y^2 \equiv ax^2 + 1 \pmod{p}$, $a > 0$ and $a \equiv 3 \pmod{4}$: We prove the following theorem.

Theorem 1. Let $a \equiv 3 \pmod{4}$ and $a > 0$.

$$\left(\frac{a}{n+2a}\right)_K = -\left(\frac{a}{n}\right)_K.$$

Proof. Because $a = 4k + 3$ and n is odd integer from $(n, 4a) = 1$, we obtain

$$\left(\frac{a}{n}\right)_K = (-1)^{\frac{a-1}{2} \cdot \frac{n-1}{2}} \left(\frac{n}{a}\right)_K = (-1)^{\frac{n-1}{2}} \left(\frac{n}{a}\right)_K,$$

from (2). While we have

$$\left(\frac{a}{n+2a}\right)_K = (-1)^{\frac{a-1}{2} \cdot \frac{n+2a-1}{2}} \left(\frac{n+2a}{a}\right)_K = (-1)^{\frac{n-1}{2} + a} \left(\frac{n}{a}\right)_K,$$

where we used (7). Then we obtain $\left(\frac{a}{n+2a}\right)_K / \left(\frac{a}{n}\right)_K = (-1)^a = -1$. ■

TABLE I: RELATION AMONG n , m AND ℓ FOR $a = 11$

m	1	2	3	4	5	6	7	8	9	10
ℓ	0	0	1	1	1	1	1	1	2	2
n	15	19	1	5	9	13	17	21	3	7

If $\tau = 1/a$, then $q_1^{2a} = -1$, we obtain

$$\left(\frac{a}{n+2a}\right)_K q_1^{n+2a} = \left(\frac{a}{n}\right)_K q_1^n.$$

The generalized Gaussian sum $f(1/a)$ repeatedly contains $\bar{f}(1/a)$ shown in the following

$$\bar{f}(1/a) = \sum_{n=1, (n,4a)=1}^{2a-1} \left(\frac{a}{n}\right)_K q_1^n = \sum_{n=1, (n,4a)=1}^{2a-1} (-1)^{\frac{n-1}{2}} \left(\frac{n}{a}\right)_K q_1^n. \quad (14)$$

In (14), n takes $(a-1)$ values as $n \in \{1, 3, \dots, \check{a}, \dots, 2a-1\}$, where \check{a} indicates that a is not included. These values can be mapped to the following values m as $m \in \{1, 2, 3, \dots, a-1\}$. The relation between n and m is given with suitable integer ℓ as follows

$$n = 4m - a(2\ell - 1). \quad (15)$$

We show here an example for $a = 11$ in the Table I. Proof for any a will be given in Appendix A. Replace n in (14) with m to get the following equation

$$\bar{f}(1/a) = \sum_{n=1, (n,4a)=1}^{2a-1} \left(\frac{n}{a}\right)_K (-1)^{\frac{n-1}{2}} q_1^n = \sum_{m=1}^{a-1} \left(\frac{4m - a(2\ell - 1)}{a}\right)_K (-1)^{\frac{4m - a(2\ell - 1) - 1}{2}} q_1^{4m - a(2\ell - 1)}. \quad (16)$$

By using (3), (5) and (7), we obtain

$$\left(\frac{4m - a(2\ell - 1)}{a}\right)_K = \left(\frac{4m}{a}\right)_K = \left(\frac{2}{a}\right)_K \left(\frac{2}{a}\right)_K \left(\frac{m}{a}\right)_K = \left(\frac{m}{a}\right)_K.$$

Furthermore, we obtain

$$(-1)^{\frac{4m - a(2\ell - 1) - 1}{2}} = (-1)^{2m - a\ell + \frac{a-1}{2}} = ((-1)^{-a})^\ell (-1)^{\frac{a-1}{2}} = (-1)^{\ell+1},$$

$$q_1^{4m - a(2\ell - 1)} = \exp(2\pi i m/a) \exp((-2\ell + 1)\pi i/2) = i(-1)^\ell \exp(2\pi i m/a),$$

where we used $q_1 = \exp(\pi i/2a)$.

If we put $a = p$ (prime number) further, $\bar{f}(1/p)$ becomes the Gaussian sum in the form

$$\bar{f}(1/p) = -i \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) \exp(2\pi i m/p) = -i G_p = \sqrt{p}, \quad p \equiv 3 \pmod{4}. \quad (17)$$

4) $y^2 \equiv ax^2 + 1 \pmod{p}$, $a < 0$ and $a \equiv 3 \pmod{4}$: We rewrite $f(\tau)$ as

$$f(\tau) = \sum_{n=1, (n,4a)=1}^{\infty} \left(\frac{-|a|}{n}\right)_K q_1^n, \quad q_1 = \exp(2\pi i \tau/4). \quad (18)$$

Theorem 2. Let $a \equiv 3 \pmod{4}$ and $a < 0$.

$$\left(\frac{-|a|}{n+2|a|}\right)_K = -\left(\frac{-|a|}{n}\right)_K.$$

Proof. $|a| \equiv 1 \pmod{4}$ and n is odd because of $(n, 4|a|) = 1$. Then $(-1)^{\frac{|a|-1}{2}} = 1$ and $\frac{n-1}{2}$ is integer. We, therefore, obtain

$$\left(\frac{-|a|}{n}\right)_K = \left(\frac{-1}{n}\right)_K \left(\frac{|a|}{n}\right)_K = (-1)^{\frac{n-1}{2}} \times (-1)^{\frac{|a|-1}{2} \cdot \frac{n-1}{2}} \left(\frac{n}{|a|}\right)_K = (-1)^{\frac{n-1}{2}} \left(\frac{n}{|a|}\right)_K.$$

While we obtain

$$\begin{aligned} \left(\frac{-|a|}{n+2|a|} \right)_K &= \left(\frac{-1}{n+2|a|} \right)_K \left(\frac{|a|}{n+2|a|} \right)_K = (-1)^{\frac{n+2|a|-1}{2}} \times (-1)^{\frac{|a|-1}{2} \cdot \frac{n+2|a|-1}{2}} \left(\frac{n+2|a|}{|a|} \right)_K \\ &= (-1)^{\frac{n+1}{2}} \left(\frac{n}{|a|} \right)_K. \end{aligned}$$

Note that $\frac{n+2|a|-1}{2} = \frac{n+1}{2} + |a| - 1$. Then we obtain

$$\left(\frac{-|a|}{n+2|a|} \right)_K \bigg/ \left(\frac{-|a|}{n} \right)_K = -1. \blacksquare$$

If $\tau = 1/|a|$, then $q_1^{2|a|} = -1$, and we obtain

$$\left(\frac{-|a|}{n+2|a|} \right)_K q_1^{n+2|a|} = \left(\frac{-|a|}{n} \right)_K q_1^n.$$

The generalized Gaussian sum $f(1/|a|)$ repeatedly contains $\bar{f}(1/|a|)$ shown in the following

$$\bar{f}(1/|a|) = \sum_{n=1, (n,4|a|)=1}^{2|a|-1} \left(\frac{-|a|}{n} \right)_K q_1^n = \sum_{n=1, (n,4|a|)=1}^{2|a|-1} (-1)^{\frac{n-1}{2}} \left(\frac{n}{|a|} \right)_K q_1^n. \quad (19)$$

$n \in \{1, 3, \dots, |a|, \dots, 2|a|-1\}$ and $m \in \{1, 2, 3, \dots, |a|-1\}$ are connected each other with suitable integer ℓ as follows

$$n = 4m - |a|(2\ell - 1).$$

This will be proved in Appendix.

By the same calculation as shown below (16), we have

$$\begin{aligned} \bar{f}(1/|a|) &= \sum_{\substack{n=1 \\ (n,4|a|)=1}}^{2|a|-1} (-1)^{\frac{n-1}{2}} \left(\frac{n}{|a|} \right)_K q_1^n \\ &= \sum_{m=1}^{|a|-1} (-1)^{\frac{4m-|a|(2\ell-1)-1}{2}} \left(\frac{4m-|a|(2\ell-1)}{|a|} \right)_K q_1^{4m-|a|(2\ell-1)} \\ &= \sum_{m=1}^{|a|-1} (-1)^\ell \left(\frac{m}{|a|} \right)_K \exp(2\pi i m/|a|) \times i(-1)^\ell \\ &= i \sum_{m=1}^{|a|-1} \left(\frac{m}{|a|} \right)_K \exp(2\pi i m/|a|), \end{aligned} \quad (20)$$

where we used $q_1 = \exp(\pi i/2|a|)$.

If we put $|a| = p$ (prime number) further, $\bar{f}(1/p)$ becomes the Gaussian sum in the form

$$\bar{f}(1/p) = i \sum_{m=1}^{p-1} \left(\frac{m}{p} \right) \exp(2\pi i m/p) = iG_p = i\sqrt{p}, \quad p \equiv 1 \pmod{4}. \quad (21)$$

5) $y^2 \equiv ax^2 + 1 \pmod{p}$, $a \equiv 2 \pmod{4}$: We put $a = 2(2k+1) = 2a'$, where a' is odd. Here n is odd integer owing to $(n, 4a) = 1$.

Theorem 3. Let $a \equiv 2 \pmod{4}$ and $a > 0$.

$$\left(\frac{a}{n+2a} \right)_K = - \left(\frac{a}{n} \right)_K.$$

Proof. (3) can be rewritten for odd n as $\left(\frac{n}{2} \right)_K = \left(\frac{2}{n} \right)_K = (-1)^{\frac{n^2-1}{8}}.$

Then we obtain

$$\begin{aligned} \left(\frac{a}{n+2a}\right)_K &= \left(\frac{2a'}{n+4a'}\right)_K = \left(\frac{2}{n+4a'}\right)_K \left(\frac{a'}{n+4a'}\right)_K = (-1)^{\frac{(n+4a')^2-1}{8}} \\ &\times (-1)^{\frac{a'-1}{2} \cdot \frac{(n+4a')-1}{2}} \left(\frac{n+4a'}{a'}\right)_K = (-1)^{\frac{n^2-1}{8}} (-1)^{na'} \times (-1)^{\frac{a'-1}{2} \cdot \frac{n-1}{2}} \left(\frac{n}{a'}\right)_K = -(-1)^{\frac{n^2-1}{8}} \\ &\times (-1)^{\frac{a'-1}{2} \cdot \frac{n-1}{2}} \left(\frac{n}{a'}\right)_K. \end{aligned}$$

While we obtain

$$\left(\frac{a}{n}\right)_K = \left(\frac{2a'}{n}\right)_K = \left(\frac{2}{n}\right)_K \left(\frac{a'}{n}\right)_K = (-1)^{\frac{n^2-1}{8}} \times (-1)^{\frac{a'-1}{2} \cdot \frac{n-1}{2}} \left(\frac{n}{a'}\right)_K.$$

Thus we obtain $\left(\frac{a}{n+2a}\right)_K / \left(\frac{a}{n}\right)_K = -1$. ■

If $\tau = 1/a$, then $q_1^{2a} = -1$, and we obtain

$$\left(\frac{a}{n+2a}\right)_K q^{n+2a} = \left(\frac{a}{n}\right)_K q^n.$$

The generalized Gaussian sum $f(1/a)$ repeatedly contains $\bar{f}(1/a)$ shown in the following

$$\bar{f}(1/a) = \sum_{n=1, (n, 4a)=1}^{2a-1} \left(\frac{a}{n}\right)_K \exp(2\pi in/4a). \quad (22)$$

In the case of $a < 0$, the similar calculation shows that

$$\bar{f}(1/|a|) = \sum_{n=1, (n, 4|a|)=1}^{2|a|-1} \left(\frac{-|a|}{n}\right)_K \exp(2\pi in/4|a|). \quad (23)$$

By using the other expression of Gaussian sum, (22) and (23) are expected to be rewritten as follows

$$\begin{aligned} \bar{f}(1/a) &= \frac{1}{1+i} \sum_{n=0}^{2a-1} \exp(2\pi in^2/4a) = \sqrt{a}, \text{ if } a > 0 \text{ and } a \equiv 2 \pmod{4}, \\ \bar{f}(1/|a|) &= \frac{i}{1+i} \sum_{n=0}^{2|a|-1} \exp(2\pi in^2/4|a|) = i\sqrt{|a|}, \text{ if } a < 0 \text{ and } a \equiv 2 \pmod{4}. \end{aligned}$$

For $a = \pm 2, \pm 6, \pm 10$, we have verified that our expectation is correct. Below, we show $a = 6$ case. With $q_1 = \exp(\pi i/12)$, we obtain

$$\sum_{n=1, (n, 24)=1}^{11} \left(\frac{6}{n}\right)_K q_1^n = q_1 + q_1^5 - q_1^7 - q_1^{11} = \sqrt{6},$$

and

$$\sum_{n=0}^{11} q_1^{n^2} = 1 + q_1 + q_1^4 + q_1^9 - q_1^4 + q_1 - 1 + q_1 - q_1^4 + q_1^9 + q_1^4 + q_1 = 4q_1 + 2q_1^9 = (1+i)\sqrt{6}.$$

2.3. Modular Transformation Structure

Here we explain the generalized Gaussian sum is associated with a theta function.

Theorem 4. *There are two expressions of the Gaussian sum in the form*

$$G_p = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \exp(2\pi in/p) = \sum_{m=0}^{p-1} \exp(2\pi im^2/p) = \sqrt{(-1)^{\frac{p-1}{2}} p}. \quad (24)$$

Proof of the second expression. We consider the quantity

$$I = \sum_{\substack{a=1, \\ a=\text{quadratic} \\ \text{residue}}}^{p-1} \exp(2\pi ia/p), \quad (25)$$

in $a \in \mathbf{F}_p^\times \cdot \{1^2, 2^2, \dots, n^2, \dots, (p-n)^2, \dots, (p-1)^2\}$ are quadratic residues, and the same quadratic residue comes twice as $n^2 \equiv (p-n)^2 \pmod{p}$. Then we have $I = \frac{1}{2} \sum_{m=1}^{p-1} \exp(2\pi i m^2/p)$. While we obtain

$$\begin{aligned} G_p &= \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) \exp(2\pi i m/p) = \sum_{\substack{a=1, \\ a=\text{quadratic} \\ \text{residue}}}^{p-1} \exp(2\pi i a/p) - \sum_{\substack{a=1, \\ a=\text{quadratic} \\ \text{non-residue}}}^{p-1} \exp(2\pi i a/p) \\ &= I - J. \end{aligned} \quad (26)$$

By the way, we obtain $I + J = \sum_{m=1}^{p-1} \exp(2\pi i m/p) = -1$, which gives $J = -I - 1$. Then we conclude

$$G_p = 2I + 1 = \sum_{m=1}^{p-1} \exp(2\pi i m^2/p) + 1 = \sum_{m=0}^{p-1} \exp(2\pi i m^2/p). \blacksquare \quad (27)$$

Thus we obtain the generalized Gaussian sum with the other expression in the form

$$G(\tau) = \sum_{n=1}^{\infty} \left(\frac{n}{p}\right) \exp(2\pi i n\tau) = \sum_{m=0}^{\infty} \exp(2\pi i m^2\tau). \quad (28)$$

Using this generalized Gaussian sum with the other expression, we can connect the generalized Gaussian sum with the elliptic theta function in the form

$$G(\tau) = 1 + \sum_{n=1}^{\infty} \exp(2\pi i n^2\tau) = \frac{1}{2} \left(\vartheta \left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix} \right] (0, \tau) + 1 \right). \quad (29)$$

The elliptic theta function has the structure of the modular transformation, and by shifting the constant value, the generalized Gaussian sum also has the structure of the modular transformation.

Through the considerations above, we conclude the generalized Gaussian sum is the quadratic curve analogue of the modular form in the Taniyama-Shimura conjecture.

3. CONCLUSION

We have examined the quadratic curve analogue of the Taniyama-Shimura conjecture for the quadratic curves. The number of solutions in \mathbf{F}_p is governed by the order of the quadratic curve analogue of the Mordell-Weil group. For quadratic curves $y^2 \equiv ax^2 + 1 \pmod{p}$, the order of the group of the Mordell-Weil analogue is given by $N(p) = p - \left(\frac{a}{p}\right)$. If we make the combination of $b(p) = p - N(p) = \left(\frac{a}{p}\right)$, we obtain

$$-b(p) = N(p) - p = \sum_{n=1}^{p-1} \left(\frac{ax^2 + 1}{p}\right). \quad (30)$$

For the quadratic curve analogue of the modular form of the Taniyama-Shimura conjecture, by replacing the Legendre symbol with the Kronecker symbol, we obtain the generalized Gaussian sum. If we use the other form of the Gaussian sum, the generalized Gaussian sum is connected with the elliptic theta function with zero argument. Thus, the generalized Gaussian sum has the structure of the modular transformation.

APPENDIX

Correspondence between $n \in \{1, 3, \dots, \check{a}, \dots, 2a-1\}$ and $m \in \{1, 2, 3, \dots, a-1\}$ for odd a .

In this appendix, we show that $n \in \{1, 3, \dots, \check{a}, \dots, 2a-1\}$ and $m \in \{1, 2, 3, \dots, a-1\}$ are mapped to each other by using the following relation with a suitable integer ℓ for odd a :

$$n = 4m - a(2\ell - 1), \quad \ell = 0, 1, 2, \dots \quad (31)$$

Theorem 5. If $m_1 \neq m_2$, then $n_1 \neq n_2$.

Proof. Let $n_1 = 4m_1 - a(2\ell_1 - 1)$ and $n_2 = 4m_2 - a(2\ell_2 - 1)$. Then

$$n_1 - n_2 = 2(2(m_1 - m_2) - a(\ell_1 - \ell_2)).$$

Suppose $n_1 = n_2$, then $2(m_1 - m_2) = a(\ell_1 - \ell_2)$. Since a is odd, $\ell_1 - \ell_2$ must be even. If $m_1 \neq m_2$, $|a(\ell_1 - \ell_2)| \geq 2a$, while $|2(m_1 - m_2)| \leq 2(a-1)$ because m_1 and m_2 are elements of $\{1, 2, 3, \dots, a-1\}$. Then, $2(m_1 - m_2) - a(\ell_1 - \ell_2)$ cannot be reduced to 0 for $m_1 \neq m_2$, which contradicts the assumption $n_1 = n_2$. Namely, we conclude that $n_1 \neq n_2$ if $m_1 \neq m_2$. ■

Theorem 6. If odd integer $n \in \{1, 3, 5, \dots, a-1\}$ is given, then $m \in \{1, 2, 3, \dots, a-1\}$ and ℓ are determined from (31).

Proof. To solve (31), we first consider the equation

$$1 = 4X + aY.$$

Thanks to $(4, a) = 1$, this equation always has an integer solution $X = X_0$ and $Y = Y_0$, where Y_0 must be odd because a is odd. By multiplying n , we obtain the solution of (31) as $m = m_0 = nX_0$ and $-2(\ell - 1) = -2(\ell_0 - 1) = nY_0$, namely

$$n = 4m_0 - a(2\ell_0 - 1).$$

It can be seen that (31) has an infinite number of solutions. Indeed, for any integer k

$$m = m_0 + ka, \quad \ell = \ell_0 + 2ka, \quad (32)$$

are solution of (31). By making k an appropriate integer, m can be an element of $\{1, 2, 3, \dots, a-1\}$ except when m is 0. If $m = 0$, however, $n = a$ with $\ell = 0$. it is the excluded value for n . The exclusion of $n = a$ follows from the fact that the definition of $\tilde{f}(\tau)$ given in (14) and (19) includes $\left(\frac{a}{n}\right)_K$, which is 0 for $n = a$. ■

CONFLICT OF INTEREST

The authors declare that they do not have any conflict of interest.

REFERENCES

- [1] Ablowitz MJ, Kaup DJ, Newell AC, Segur H. Nonlinear-evolution equations of physical significance. *Phys Rev Lett.* 1973;31:125–7. doi: 10.1103/PhysRevLett.31.125.
- [2] Bianchi L. Ricerche sulle superficie elicoidali e sulle superficie a curvatura costante. *Ann Scuola Norm Sup Pisa.* 1879;2(1):285–341. Available from: <http://eudml.org/doc/82743>.
- [3] Crampin M. Solitons and SL(2,R). *Phys Lett.* 1978;A66:170–2. doi: 10.1016/0375-9601(78)90646-1.
- [4] Hermann R. Pseudopotentials of Estabrook and Wahlquist. The geometry of solitons, and the theory of connections. *Phys Rev Lett.* 1976;36:835–6. doi: 10.1103/PhysRevLett.36.835.
- [5] Sasaki R. Soliton equation and pseudospherical surfaces. *Nucl Phys.* 1979;B154:343–57. doi: 10.1016/0550-3213(79)90517-0.
- [6] Hayashi M, Shigemoto K, Tsukioka T. The half-period addition formulae for genus two hyperelliptic \wp functions and the $\text{Sp}(4, \mathbb{R})$ lie group structure. *J Phys Commun.* 2022;6:085004. doi: 10.1088/2399-6528/ac8521.
- [7] Breuil C, Conrad B, Diamond F, Taylor R. On the modularity of elliptic curves over \mathbb{Q} : wild 3-Adic exercises. *J Amer Math Soc.* 2001;14:843–939. doi: 10.1090/S0894-0347-99-00287-8.
- [8] Eichler M. Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion. *Archiv für mathematische Logik und Grundlagenforschung.* 1954;5:355–66. doi: 10.1007/BF01898377.
- [9] Shimura G. Correspondances modulaires et les fonctions ζ de courbes algébriques. *J Math Soc Japan.* 1958;10:1–28. doi: 10.2969/jmsj/01010001.
- [10] Mordell LJ. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc Camb Phil Soc.* 1922;21:179–82.
- [11] Weil A. L'arithmétique sur les courbes algébriques. *Acta Math.* 1929;52:281–315. doi: 10.1007/BF02592688.