$SL_2(\mathcal{F}q)$---REPRESENTATIONS

OF TORUS KNOTS

By

LIANG XU

Bachelor of Science

Hubei University

Wuhan, Hubei

People's Republic of China

1995

Submitted to the Faculty of the
Graduate College of
Oklahoma State University
in partial fulfillment of
the requirement for
the Degree of
MASTER OF SCIENCE
August, 2001

$SL_2(\mathcal{F}q)$---REPRESENTATIONS

OF TORUS KNOTS

Thesis Approved:

Weiping Li

Thesis Advisor

James W Cogdell

Roger Zierau

Alfred Carlozzi

Dean of the Graduate College

ACKNOWLEDGEMENTS

I wish to express my sincere appreciate to my advisor, Dr. Weiping Li for inspiration, encouragement, and constructive guidance about the thesis, because without him this would not be possible.

Special thanks are extended to Dr. Jim Cogdell and Dr. Roger Zierau for kindly agreeing to serve on my committee.

I would also like to express my thanks to my friends and parents, for their support and love during these years.

Finally, I would like to thank the Department of Mathematics in OSU for supporting during these one and a half years.

TABLE OF CONTENTS

LIST OF TABLES

1. Introduction

The Casson invariant defined in [1] was originally an invariant of integral homology 3-spheres, and it was extended to an invariant of knots in integral homology 3-spheres through surgery relations. The intrinsic extension of the Casson invariant for knots was developed in [5] and generalized to the sympelctic Floer homology in [3]. The Casson-Lin invariant defined in [3, 5] was an invariant of knots as roughly counting irreducible $SU(2)$-representations of the knot groups with trace-zero along all meridians.

There is an attempt to define a characteristic-p Casson invariant in [7]. One would like to have the characteristic-p Casson invariant preserving all properties of the Casson invariant in [1, 3, 5]. Thus one can count representations of the knot group into $SL_2(\mathcal{F}_q)$, where F_q is a finite field and $q = p^s$. Note that the finite field version of $SU(2)$ does not have the some nice property as $SU(2)$, and the Lie algebras of $SU(2)$ and $SL_2(C)$ are pretty much the same as isomorphism. In [4], the $SL_2(C)$ knot invariant was studied and the relation with $SU(2)$ knot invariant is discovered.

For finite field case, instead of representation varieties, there is no nice intersection pairing since the representation spaces are not projective. Thus one simply count the representations of knot groups into $SL_2(\mathcal{F}_q)$. Our work is motivated by the study of Sink [7]. We use some explicit methods to count the representations of (n, m) torus knot. Our main results can be stated in the following.

Theorem 1.1. *There is a formula to compute the number of representations of $(n, 2)$ torus knot into $SL_2(\mathcal{F}_q)$ up to conjugacy (see Table III).*

Our formula in Table III has a discrepancy with the result in [7]. We compute some explicit solutions to show that there are errors in the counting of [7] in §3.

Using the numbers of representations we counted in §2, we formulate a zeta function of the numbers of representations of $SL_2(\mathcal{F}_q)$ where $q = p^s$ for $s \in N$. The zeta function of the $(n, 2)$ torus knot can be computed in an explicit manner. Then we can verify the modified zeta function λ_K^{-2} is a polynomial for n prime, or a product of two primes, or a square of a prime. We expect this phenomena true for general n as it was claimed in Theorem 3 of [7].

The thesis is organized as follows: we first review the conjugacy classes and stabilizers in $SL_2(\mathcal{F}_q)$ in §2.1. Few elementary number theoretic countings and cyclic group properties are presented in §2.2. In §2.3, we start to counting the number of representations of $(n, 2)$ torus knot group into $SL_2(\mathcal{F}_q)$ up to conjugacy and prove Theorem 1.1. We give two counterexamples to statements in [7] in §3. In §4, we study the Zeta function of $(n, 2)$ torus knot and verify that the modified Zeta function λ_K^{-2} is a polynomial for some special cases.

2. First Method for $(n, 2)$ torus knot

We will count representations $SL_2(\mathcal{F}_q)$ of the fundamental group G of the $(n, 2)$ torus knot up to conjugacy, where $\mathcal{F}_q$ is a finite field with $q = p^s$ for a prime number $p > 2$. As we know, the fundamental group of $(n, 2)$ torus knot can be presented by

$< a, b | a^n = b^2 >$. Any representation $\rho : G \to SL_2(\mathcal{F}_q)$ can be one-to-one identified with $(\rho(a), \rho(b)) \in SL_2(\mathcal{F}_q) \times SL_2(\mathcal{F}_q)$ such that $\rho(a)^n = \rho(b)^2$. Hence we have the correspondence between a representation and a pair (A, B) of $SL_2(\mathcal{F}_q)$ matrices with $A^n = B^2$. Since we count the representations up to conjugacy and we can always conjugate one of A and B into a standard representative of one of the conjugacy classes, we may choose A to be the element and find the number of B satisfying $A^n = B^2$.

2.1. **Conjugacy Classes in $SL_2(\mathcal{F}_q)$.** We have to find the conjugacy classes in $SL_2(\mathcal{F}_q)$, and this is well-known in [2], and see Table I. Let ϵ be an element of $\mathcal{F}_q$ with $\sqrt{\epsilon} \notin \mathcal{F}_q$.

Table I

Case No.	**Representative**	**No. of Elts in Class**	**No. Classes**
1.	$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	1	1
2.	$-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	1	1
3.	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\frac{q^2-1}{2}$	1
4.	$\begin{pmatrix} 1 & \epsilon \\ 0 & 1 \end{pmatrix}$	$\frac{q^2-1}{2}$	1
5.	$\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$	$\frac{q^2-1}{2}$	1
6.	$\begin{pmatrix} -1 & \epsilon \\ 0 & -1 \end{pmatrix}$	$\frac{q^2-1}{2}$	1
7.	$\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}$	$q(q+1)$	$\frac{q-3}{2}$
8.	$\begin{pmatrix} x & y \\ \epsilon y & x \end{pmatrix}$	$q(q-1)$	$\frac{q-1}{2}$

Note that we have certain redundancies in the above table; namely in Case 7, the matrices $\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}$ and $\begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix}$ are in the same conjugacy class. Also in that same Case 7, we do not allow x to be ± 1 since they are covered in Case 1 and Case

2 respectively. Also, in Case 8, the matrix $\begin{pmatrix} x & y \\ \epsilon y & x \end{pmatrix}$ is conjugate to the matrix $\begin{pmatrix} x & -y \\ \epsilon y & x \end{pmatrix}$ and further cannot let $y = 0$, otherwise it reduces to Case 1 or 2.

The following table gives the group of stabilizers for each case.

Table II

Case No.	**The stabilizer of each representative in $SL_2(\mathcal{F}_q)$**
1.	$SL_2(\mathcal{F}_q)$
2.	$SL_2(\mathcal{F}_q)$
3.	$\{\begin{pmatrix} \pm 1 & x \\ 0 & \pm 1 \end{pmatrix} \mid x \in \mathcal{F}_q\}$
4.	$\{\begin{pmatrix} \pm 1 & x \\ 0 & \pm 1 \end{pmatrix} \mid x \in \mathcal{F}_q\}$
5.	$\{\begin{pmatrix} \pm 1 & x \\ 0 & \pm 1 \end{pmatrix} \mid x \in \mathcal{F}_q\}$
6.	$\{\begin{pmatrix} \pm 1 & x \\ 0 & \pm 1 \end{pmatrix} \mid x \in \mathcal{F}_q\}$
7.	$\{\begin{pmatrix} y & 0 \\ 0 & y^{-1} \end{pmatrix} \mid y \in \mathcal{F}_q - 0\}$
8.	$\{\begin{pmatrix} a & b \\ \epsilon b & a \end{pmatrix} \mid a^2 - \epsilon b^2 = 1\}$

We list the characteristic polynomials for each case. For Case 1, Case 3 and Case 4, the characteristic polynomial is $\lambda^2 - 2\lambda + 1 = 0$. For Case 2, Case 5 and Case 6, the characteristic polynomial is $\lambda^2 + 2\lambda + 1 = 0$. For Case 7, the characteristic polynomial is $\lambda^2 - (x + x^{-1})\lambda + 1 = 0$. For Case 8, the characteristic polynomial is $\lambda^2 - 2x\lambda + 1 = 0$.

In the following paper, we use C_A to be the set of the elements conjugate to A in $SL_2(\mathcal{F}_q)$ and use Γ_A to be the stabilizer of A.

2.2. **Preliminary Results.** Before we begin to discuss solutions of each case, let us give elementary propositions which we will use later.

Proposition 2.1. *Let a, b and m be integers such that $m > 0$ and $(a, m) = d$, where (a, m) is the greatest common divisor of a and m. If $d \nmid b$, then $ax \equiv b \pmod{m}$*

has no solutions. If $d \mid b$, then $ax \equiv b \pmod{m}$ has exactly d incongruent solutions modulo m.

The proposition is important to prove the following propositions and it is in Section 4.9 of [6].

Proposition 2.2. *Given a finite cyclic group G, $|G| = m$, where $|\cdot|$ is the cardinality. Let $G^n = \{x^n | x \in G\}$. For a $y \in G^n$, the number of solutions for $x^n = y$ is (m, n).*

Proof. Since G is a cyclic group, let g be the generator of G. Then there exists a t with $0 \leq t < m - 1$, such that $g^t = y$. Write $x = g^s$ for some s. Then the equation $x^n = y$ is reduced to the equation $ns \equiv t \pmod{m}$. Clearly there exists a solution for $ns \equiv t \pmod{m}$ since $y \in G^n$. By Proposition 2.1, it has (n, m) solutions. $\square$

Proposition 2.3. *For a finite cyclic group G, let $|G| = m$, then $|G^n| = \frac{m}{(m,n)}$.*

Proof. It is clear that $|G^n| * |\{x \in G | x^n = y \text{ with } y \in G^n\}| = |G|$. By Proposition 2.2, $|G^n| = \frac{m}{(n,m)}$. $\square$

Proposition 2.4. *For a finite field $\mathcal{F}_q$, G is cyclic subgroup of $\mathcal{F}_q$ with respect to multiplication with $-1 \in G$. Let m be even. Then there is a solution for the equation $x^m = -1$ in G if and only if $(m, |G|) | \frac{|G|}{2}$.*

Proof. Let g be the generator of the cyclic group G. Clearly $g^{|G|} = 1$ and $(-1)^2 = 1$. Let $g^t = -1$ with $0 < t < |G|$. Then $g^{2t} = 1$ which means $2t = |G|$, i.e., $g^{\frac{|G|}{2}} = -1$.

Like the discussion in the proof of Proposition 2.2, to solve the equation $x^m = -1$ is equivalent to solve the equation $sm \equiv \frac{|G|}{2} \pmod{|G|}$. By Proposition 2.1, there is a solution for equation $x^m = -1$ in G if and only if $(m, |G|) | \frac{|G|}{2}$. $\square$

Proposition 2.5. *For a finite field $\mathcal{F}_q$, then if $q \equiv 1 \pmod{4}$, then there are two solutions for the equation $x^2 = -1$ in the $\mathcal{F}_q$. If $q \equiv 3 \pmod{4}$, then there is no solution for the equation $x^2 = -1$ in the $\mathcal{F}_q$.*

Proof. To determine whether there is a solution for $x^2 = -1$ is equivalent to find a solution in $\mathcal{F}_q - 0$, which is a cyclic group with respect to multiplication. By Proposition 2.4, there exists a solution for $x^2 = -1$ in $\mathcal{F}_q$ if and only if $(2, q-1) | \frac{q-1}{2}$. Therefore if $q \equiv 1 \pmod{4}$, then there are two solutions for the equation $x^2 = -1$ in the $\mathcal{F}_q$. If $q \equiv 3 \pmod{4}$, then there is no solution for the equation $x^2 = -1$ in the $\mathcal{F}_q$. $\square$

Proposition 2.6. *The set $\Omega = \{\begin{pmatrix} x & y \\ \epsilon y & x \end{pmatrix} | \begin{pmatrix} x & y \\ \epsilon y & x \end{pmatrix} \in SL_2(\mathcal{F}_q)\}$ is a cyclic group. Let $\mathcal{F}'$ be the vector space over $\mathcal{F}_q$ with the basis 1 and $\sqrt{\epsilon}$. Let $C = \{\varsigma \in (\mathcal{F}\prime)^* | \varsigma^{q+1} = 1\}$. Let $\phi : \Omega \to C$ be $\phi(\begin{pmatrix} x & y \\ \epsilon y & x \end{pmatrix}) = x + \sqrt{\epsilon} y$. Then ϕ is a isomorphism, and $|\Omega| = |C| = q + 1$.*

The statement is shown in Chapter 5 of [2].

For the convenience of the discussion, we let $\Omega_1 = \Omega - \{\pm I\}$.

Proposition 2.7. *For the cyclic group Ω as we defined in Proposition 2.6, if $q \equiv 1 \pmod 4$, there is no solution for the equation $A^2 = -I$. If $q \equiv 3 \pmod 4$, there are two solutions for the equation $A^2 = -I$, where $A \in \Omega$.*

Proof. Clearly $-I \in \Omega$. By Proposition 2.6, $|\Omega| = q+1$. By Proposition 2.4, there is a solution for $A^2 = -I$ if and only if $(2, q+1)|\frac{q+1}{2}$. Therefore if $q \equiv 1 \pmod 4$, there is no solution for the equation $A^2 = -I$. If $q \equiv 3 \pmod 4$, there are two solutions for the equation $A^2 = -I$, where $A \in \Omega$. □

Proposition 2.8. *Let p, q be coprime natural numbers. Suppose that the equation $p^x \equiv -1 \pmod q$ has solutions. Let m_0 be the smallest positive solution of the equation. If m is another solution for $p^x \equiv -1 \pmod q$, then $m = km_0$ for some positive odd integer k.*

Proof. Note by Fermat's little theorem, there exists a solution for $p^x \equiv 1 \pmod q$. Let m_1 be the smallest positive solution for $p^x \equiv 1 \pmod q$. First we show $m_1 > m_0$. Otherwise there exist a and b such that $m_0 = am_1 + b$ with $a \geq 1$ and $0 < b < m_1 < m_0$. Therefore $p^b \equiv -1 \pmod q$ which is contradictory to the assumption of m_0 is the smallest positive solution of $p^x \equiv -1 \pmod q$. Clearly $p^{lm_0} \equiv q \pmod q$ for some even number l. So if $m_0|m$, then $m = km_0$ for some odd integer k.

Assume $m_0 \nmid m$, there exist positive integers c and d such that $m = cm_0 + d$ with $0 < d < m_0$. If c is even, then we get $p^d \equiv -1 \pmod q$, which is impossible. If c is odd, then we get $p^d \equiv 1 \pmod 1$, but $d < m_0 < m_1$, so it is false. Therefore $m_0|m$. □

Proposition 2.9. *For a finite field $\mathcal{F}_q$, if x is in $\mathcal{F}_q$ with $\sqrt{x} \notin \mathcal{F}_q$, then $\sqrt{x^{-1}} \notin \mathcal{F}_q$. If the square root of both x and y are not in $\mathcal{F}_q$, then $\sqrt{xy} \in \mathcal{F}_q$.*

Proof. Let g be the generator of the cyclic group $\mathcal{F}_q - 0$ with respect to multiplication. Since $\sqrt{x} \notin \mathcal{F}_q$, $x = g^s$ for some odd number s. Clearly $x^{-1} = g^{q-1-s}$, then $\sqrt{x^{-1}} \notin \mathcal{F}_q$. Let $y = g^t$. By the same reason, t is odd too. We get $xy = g^{s+t}$, so $\sqrt{xy} \in \mathcal{F}_q$.

Proposition 2.10. *Given A, B be representatives of different conjugate classes such that $\Gamma_A \cap \Gamma_B = \{\pm I\}$. For a $G \in SL_2(\mathcal{F}_q)$, let $B_1 = GBG^{-1}$. Then $\Gamma_A \cap \Gamma_{B_1} = \{\pm I\}$.*

Proof The pair of (A, B) has the following possibilities:

1) A in Case 3, B in Case 7;

2) A in Case 3, B in Case 8;

3) A in Case 4, B in Case 7;

4) A in Case 4, B in Case 8;

5) A in Case 5, B in Case 7;

6) A in Case 5, B in Case 8;

7) A in Case 6, B in Case 7;

8) A in Case 6, B in Case 8;

9) A in Case 7, B in Case 8;

Clearly $\Gamma_{B_1} = G\Gamma_B G^{-1}$. Given $C \in \Gamma_A$, $D \in \Gamma_{B_1}$ such that C and $D \neq \pm I$. By Table II, C and D have different characteristic polynomials. Clearly $\{\pm I\} \subset \Gamma_A \cap \Gamma_{B_1}$. Therefore $\Gamma_A \cap \Gamma_{B_1} = \{\pm I\}$. $\square$

Proposition 2.11. *(1) Let* $B_0 = \begin{pmatrix} x_0 & 0 \\ 0 & x_0^{-1} \end{pmatrix}$ *with* $x_0 \neq \pm 1$ *and* $C = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathcal{F}_q)$. *If* CB_0C^{-1} *is diagonal, then* C *must be* $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ *or* $\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}$ *and* $CB_0C^{-1} = B_0^{\pm 1}$.

(2) If CB_0C^{-1} *is not diagonal, then* $\Gamma_{CB_0C^{-1}} \cap \Gamma_{B_0} = \{\pm I\}$.

Proof. (1) By a simple calculation

$$C \begin{pmatrix} x & 0 \\ 0 & x_0^{-1} \end{pmatrix} C^{-1} = \begin{pmatrix} adx_0 - bcx_0^{-1} & -ab(x_0 - x_0^{-1}) \\ cd(x_0 - x_0^{-1}) & -bcx_0 + adx_0^{-1} \end{pmatrix}.$$

Since $x_0 \neq \pm 1$, $C \begin{pmatrix} x_0 & 0 \\ 0 & x_0^{-1} \end{pmatrix} C^{-1}$ is diagonal if and only if $a = 0, d = 0$ or $b = 0, c = 0$. If $C = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$, then $CB_0C^{-1} = B_0$. If $C = \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}$, then $CB_0C^{-1} = B_0^{-1}$.

(2) Since CB_0C^{-1} is not diagonal, C cannot be in the form of (1). Note that $\Gamma_{CB_0C^{-1}} = C\Gamma_{B_0}C^{-1}$. For any $\begin{pmatrix} y & 0 \\ 0 & y^{-1} \end{pmatrix} \in \Gamma_{B_0}$ with $y \neq \pm 1$, $C \begin{pmatrix} y & 0 \\ 0 & y^{-1} \end{pmatrix} C^{-1}$ is not diagonal. Hence $\Gamma_{CB_0C^{-1}} \cap \Gamma_{B_0} = \pm I$. $\square$

Proposition 2.12. *(1) Let* $B_0 = \begin{pmatrix} x & y \\ \epsilon y & x \end{pmatrix}$ *with* $y \neq 0$, $C = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathcal{F}_q)$. *If* $B = CB_0C^{-1} \in \Omega$, *then* $C \in \Omega$ *or* $C = \begin{pmatrix} a & b \\ -\epsilon b & -a \end{pmatrix}$, *and* $B = B_0^{\pm 1}$.

(2) If $B \notin \Omega$, *then* $\Gamma_B \cap \Gamma_{B_0} = \{\pm I\}$.

Proof. (1) By a simple calculation, we get

$$C \begin{pmatrix} x & y \\ \epsilon y & x \end{pmatrix} C^{-1} = \begin{pmatrix} x + bd\epsilon y - acy & a^2 y - b^2 \epsilon y \\ \epsilon d^2 y - c^2 y & x + acy - \epsilon bdy \end{pmatrix}.$$

If $C \begin{pmatrix} x & y \\ \epsilon y & x \end{pmatrix} C^{-1} \in \Omega$, then $x + bc\epsilon y - acy = x + acy - \epsilon bdy$, which implies $(ac - \epsilon bd)y = 0$. Since $y \neq 0$, we get $ac - \epsilon bd = 0$. Therefore $a^2 - b^2\epsilon = \pm 1$. Combining with $ad - bc = 1$ and $ac - \epsilon bd = 0$, we get $a = d$, $c = \epsilon b$, i.e, $C \in \Omega$;

or $a = -d$, $c = -\epsilon b$. If $C = \begin{pmatrix} a & b \\ \epsilon b & a \end{pmatrix}$, then $CB_0C^{-1} = B$. If $C = \begin{pmatrix} a & b \\ -\epsilon b & -a \end{pmatrix}$, $CB_0C^{-1} = B_0^{-1}$.

(2) If $B \notin \Omega$, then C cannot be in form of (1). Note that $\Gamma_B = C\Gamma_{B_0}C^{-1}$. For any $A = \begin{pmatrix} u & v \\ \epsilon v & u \end{pmatrix} \in \Gamma_{B_0}$ with $v \neq 0$, $CAC^{-1} \notin \Omega$. Hence $\Gamma_B \cap \Gamma_{B_0} = \{\pm I\}$. $\square$

2.3. **Counting the Number of Solutions.** As we have said, we take the matrix A to be in the standard form of each case shown in Table I, and count the solutions B of the equation

$$A^n = B^2 \tag{1}$$

up to conjugacy in each case. It is obvious that Equation (1) is equivalent to the equation

$$A^n B^{-1} = B. \tag{2}$$

In the first 7 cases, we count solutions of Equation (2) instead of solving Equation (1) directly. In this section, we write $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with

$$ad - bc = 1 \tag{3}$$

in $\mathcal{F}_q$. Clearly $B^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Notice that $(n, 2) = 1$, so n is always odd in this section. Now we discuss the number of solutions of Equation (1) case by case.

In order to get the number of representations up to conjugacy, we need to modulo more from the stabilizers of A and B. Let $\Gamma_A = \{G \in SL_2(\mathcal{F}_q) | GAG^{-1} = A\}$ be the stabilizer of A. Hence any element $G \in \Gamma_A$ acts on (A, B) as a single conjugacy orbit (A, GBG^{-1}) with fixed conjugacy representative of A. This only affects solutions (A, B_1) and (A, B_2) with B_1 and B_2 in the same conjugacy class under Γ_A.

Case 1. Let $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Then $A^n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, Equation(2) is reduced to $B^{-1} = B$, i.e.,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}. \tag{4}$$

Therefore $d = a, b = -b$, and $c = -c$. Then $b = c = 0$. Combining with equation (3), we get $a^2 = ad = 1$ which has solutions $a = \pm 1$. Therefore we have two solutions for $B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

Note that for both two solutions of (A, B), we have $\Gamma_A = \Gamma_B = SL_2(\mathcal{F}_q)$. Hence there are two distinct solutions of $I = B^2$ up to conjugacy.

Case 2. Let $A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Then $A^n = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Equation (2) becomes

$$\begin{pmatrix} -d & b \\ c & -a \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tag{5}$$

which is equivalent to $a = -d$. Combining with equation (3), we get $d^2 + bc = -1$. There are two subcases: (a) $bc = 0$, (b) $bc \neq 0$. We count the number of solutions for each subcase and add them up.

2.a: For $bc = 0$, it is clear that

$$|\{(b,c,d)|d^2 + bc = -1, bc = 0\}| = |\{(b,c)|bc = 0\}| * |\{d|d^2 = -1\}|.$$

There are 2q-1 solutions in $\mathcal{F}_q$ for $bc = 0$. For the equation $d^2 = -1$, by Proposition 2.5, there are two solutions for $d^2 = -1$ if $q \equiv 1 \pmod 4$, and there is no solution for $d^2 = -1$ if $q \equiv 3 \pmod 4$. Therefore the number of solutions for $d^2 + bc = -1$ with $bc = 0$ in $\mathcal{F}_q$ is

$$\begin{cases} 2(2q-1) & \text{if } q \equiv 1 \pmod 4, \\ 0 & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

2.b: For $bc \neq 0$, we get the following relation

$$|\{(b,c,d)|d^2 + bc = 1, bc \neq 0\}| = |\{d|d^2 \neq -1\}| * |\{b|b \neq 0\}|.$$

According to Proposition 2.5, we have $|\{d|d^2 \neq -1\}| = q-2$ if $q \equiv 1 \pmod 4$, and $|\{d|d^2 \neq -1\}| = q$ if $q \equiv 3 \pmod 4$. Obviously $|\{b|b \neq 0\}| = q-1$. Hence the number of solutions for $d^2 - bc = -1$ with $bc \neq 0$ is

$$\begin{cases} (q-2)(q-1) & \text{if } q \equiv 1 \pmod 4, \\ q(q-1) & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

Summarizing the previous discussions, the number of solutions of Equation (1) in Case 2 is

$$\begin{cases} q(q+1) & \text{if } q \equiv 1 \pmod 4, \\ q(q-1) & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

For all the solutions B satisfying $B^2 = -I$, $B = \begin{pmatrix} -d & b \\ c & d \end{pmatrix}$ with $d^2 + bc = -1$, then its characteristic polynomial is $\lambda^2 = -1$. By the characteristic polynomial of $SL_2(\mathcal{F}_q)$, the solution must be in Case 7 or Case 8 for $x + x^{-1} = 0$ or $2x = 0$.

If $q \equiv 1 \pmod 4$, then $\sqrt{-1} \in SL_2(\mathcal{F}_q)$ by Proposition 2.5. Hence $x + x^{-1} = 0$ has a solution, all the solutions are conjugate $B_0 = \begin{pmatrix} x_0 & 0 \\ 0 & x_0^{-1} \end{pmatrix}$ with the fixed x_0 and $x_0^2 = -1$.

Let $C_{B_0} = \{GB_0G^{-1}|G \in SL_2(\mathcal{F}_q)\}$. Since B_0 is a solution for $B^2 = -I$, any element in C_{B_0} is also a solution. Therefore the collection of the solutions of $B^2 = -I$ is equal to C_{B_0}. We can write all the solutions in this case as $(-I, GB_0G^{-1})$ for some

$G \in SL_2(\mathcal{F}_q)$. On the other hand the stabilizer of $-I$ is $SL_2(\mathcal{F}_q)$. Therefore up to conjugacy, we only have one solution $(-I, \begin{pmatrix} x_0 & 0 \\ 0 & x_0^{-1} \end{pmatrix})$.

If $q \equiv 3 \pmod 4$, then $\sqrt{-1} \notin \mathcal{F}_q$ by Proposition 2.5. There is no solution for $x+x^{-1} = 0$. So all the solutions must be in Case 8. By Proposition 2.9, $\sqrt{-\epsilon^{-1}} \in \mathcal{F}_q$. Therefore all the solutions are conjugate to the matrix $B_0' = \begin{pmatrix} 0 & \sqrt{-\epsilon^{-1}} \\ \epsilon\sqrt{-\epsilon^{-1}} & 0 \end{pmatrix}$.

Let $\mathcal{C}_{B_0'} = \{GB_0'G^{-1} | G \in SL_2(\mathcal{F}_q)\}$. We can write all the solutions in this case as $(-I, GB_0'G^{-1})$ for $G \in SL_2(\mathcal{F}_q)$. For $\Gamma_{-I} = SL_2(\mathcal{F}_q)$, up to conjugacy we only have one solution $(-I, \begin{pmatrix} 0 & \sqrt{-\epsilon^{-1}} \\ \epsilon\sqrt{-\epsilon^{-1}} & 0 \end{pmatrix})$.

Therefore in Case 2, up to conjugacy the number of solutions is 1.

Case 3. Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Then $A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. Equation (2) becomes

$$A^n B^{-1} = \begin{pmatrix} d - nc & -b + an \\ -c & a \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{6}$$

One has the equivalent relations:

$$\begin{cases} d - nc = a \\ -b + an = b \\ -c = c \\ a = d. \end{cases}$$

By $-c = c$, we get $c = 0$. Combining equation (3) and $a = d$, we have $a^2 = 1$ which has solutions $a = \pm 1$. Thus $-b + an = b$ is reduced to $b = \pm 2^{-1} n$. Therefore we have two solutions in this case, i.e.,

$$B = \begin{pmatrix} \pm 1 & \pm 2^{-1} n \\ 0 & \pm 1 \end{pmatrix}.$$

Clearly $\begin{pmatrix} 1 & 2^{-1}n \\ 0 & 1 \end{pmatrix}$ cannot be conjugate to $\begin{pmatrix} -1 & -2^{-1}n \\ 0 & -1 \end{pmatrix}$ in $SL_2(\mathcal{F}_q)$ for they have different eigenvalues. Therefore we have two distinct solutions in this case.

Case 4. Let $A = \begin{pmatrix} 1 & \epsilon \\ 0 & 1 \end{pmatrix}$. Then $A^n = \begin{pmatrix} 1 & n\epsilon \\ 0 & 1 \end{pmatrix}$. Equation (2) is equivalent to

$$A^n B^{-1} = \begin{pmatrix} d - nc\epsilon & -b + an\epsilon \\ -c & a \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{7}$$

One has the equivalent relations:

$$\begin{cases} d - nc\epsilon = a \\ -b + an\epsilon = b \\ -c = c \\ a = d. \end{cases}$$

Similarly as Case 3, we get $c = 0$ from $-c = c$. Combining equation (3) and $a = d$, we have $a^2 = 1$ which has solutions $a = \pm 1$. Thus $-b + an\epsilon = b$ is reduced to $b = \pm 2^{-1} n\epsilon$.

In this case the solutions are

$$B = \begin{pmatrix} \pm 1 & \pm 2^{-1} n\epsilon \\ 0 & \pm 1 \end{pmatrix}.$$

Clearly $\begin{pmatrix} 1 & 2^{-1} n\epsilon \\ 0 & 1 \end{pmatrix}$ is not conjugate to $\begin{pmatrix} -1 & -2^{-1} n\epsilon \\ 0 & -1 \end{pmatrix}$ in $SL_2(\mathcal{F}_q)$ since they have different eigenvalues. Therefore we have two distinct solutions in this case.

Case 5. Let $A = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$. Then $A^n = \begin{pmatrix} -1 & n \\ 0 & -1 \end{pmatrix}$. Equation (2) becomes

$$A^n B^{-1} = \begin{pmatrix} -d-nc & b+an \\ c & -a \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{8}$$

One has the equivalent relations:

$$\begin{cases} -d-nc = a \\ b+an = b \\ c = c \\ -a = d. \end{cases}$$

From $b + an = b$ we get $an = 0$. If $p \nmid n$, a must be 0. Combining $-d - nc = a$ and $-a = d$, we get $c = 0$, which contradicts to the assumption $ad - bc = 1$. Therefore there is no solution.

If $p \mid n$, then $A^n = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

If $q \equiv 1 \pmod 4$, by Case 2, all the solutions can be written as (A, GB_0G^{-1}) where $B_0 = \begin{pmatrix} x_0 & 0 \\ 0 & x_0^{-1} \end{pmatrix}$ and $G \in SL_2(\mathcal{F}_q)$.

We define an action Γ_A on $\mathcal{C}_{B_0}$: $\Gamma_A \times \mathcal{C}_B \to \mathcal{C}_B$ by $(H, B) \to HBH^{-1}$ where $H \in \Gamma_A$ and $B \in \mathcal{C}_B$. Now we just need to count the orbits under the action of Γ_A. Clearly $|\Gamma_A(B)| = |\Gamma_A/\Gamma_A \cap \Gamma_B|$.

According to Table II, $\Gamma_A = \{\begin{pmatrix} \pm 1 & x \\ 0 & \pm 1 \end{pmatrix} | x \in \mathcal{F}_q\}$, and $\Gamma_{B_0} = \{\begin{pmatrix} y & 0 \\ 0 & y^{-1} \end{pmatrix} | y \in \mathcal{F}_q - 0\}$, and $\Gamma_A \cap \Gamma_{B_0} = \{\pm I\}$. For any $B = GB_0G^{-1}$, by Proposition 2.10, $\Gamma_A \cap \Gamma_B = \{\pm I\}$. Therefore $|\Gamma_A(B)| = |\Gamma_A/\Gamma_A \cap \Gamma_B| = q$ for every $B \in \mathcal{C}_{B_0}$. Since $|\mathcal{C}_{B_0}| = q(q+1)$, the number of orbits under the action of Γ_A is $q+1$. Therefore up to conjugacy the number of solutions is $q+1$.

If $q \equiv 3 \pmod 4$, by Case 2, all the solutions for $B^2 = -I$ are conjugate to $B_0' = \begin{pmatrix} 0 & \sqrt{-\epsilon^{-1}} \\ \epsilon\sqrt{-\epsilon^{-1}} & 0 \end{pmatrix}$. According to Table II, $\Gamma_A = \{\begin{pmatrix} \pm 1 & x \\ 0 & \pm 1 \end{pmatrix} | x \in \mathcal{F}_q\}$, $\Gamma_{B_0'} = \{\begin{pmatrix} x & y \\ \epsilon y & x \end{pmatrix} | x^2 - \epsilon y^2 = 1\}$, $\Gamma_A \cap \Gamma_{B_0'} = \{\pm I\}$. By the same discussion as above, we get the number of solutions up to conjugacy is $q-1$.

Thus the number of solutions of equation (1) is

$$\begin{cases} q+1 & \text{if } q \equiv 1 \pmod 4 \text{ and } p \mid n, \\ q-1 & \text{if } q \equiv 3 \pmod 4 \text{ and } p \mid n, \\ 0 & \text{Otherwise.} \end{cases}$$

Case 6. Let $A = \begin{pmatrix} -1 & \epsilon \\ 0 & -1 \end{pmatrix}$. Then $A^n = \begin{pmatrix} -1 & n\epsilon \\ 0 & -1 \end{pmatrix}$. Equation (2) becomes

$$A^n B^{-1} = \begin{pmatrix} -d - nc\epsilon & b + an\epsilon \\ c & -a \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{9}$$

One has the equivalent relations:

$$\begin{cases} -d - nc\epsilon = a \\ b + an\epsilon = b \\ c = c \\ -a = d. \end{cases}$$

From $b + an\epsilon = b$ we get $an\epsilon = 0$. With the same method as in Case 5, if $p \nmid n$, then there is no solution. If $p \mid n$, then $A^n = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. By the same discussion of Case 5, the number of solutions of equation (1) is

$$\begin{cases} q+1 & \text{if } q \equiv 1 \pmod 4 \text{ and } p \mid n, \\ q-1 & \text{if } q \equiv 3 \pmod 4 \text{ and } p \mid n, \\ 0 & \text{Otherwise.} \end{cases}$$

Case 7. Let $A = \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}, x \neq \pm 1$. Then $A^n = \begin{pmatrix} x^n & 0 \\ 0 & x^{-n} \end{pmatrix}$. Equation (2) is reduced to

$$A^n B^{-1} = \begin{pmatrix} dx^n & -bx^n \\ -cx^{-n} & ax^{-n} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{10}$$

One has the equivalent relations

$$\begin{cases} dx^n = a \\ -bx^n = b \\ -cx^{-n} = c \\ ax^{-n} = d. \end{cases}$$

From $(1+x^n)c = (1+x^n)b = 0$, Equation (10) is split to two subcases, (a) $1+x^n = 0$, (b)$1 + x^n \neq 0$.

7.a: For $1 + x^n = 0$, we have $A^n = -I$. It is clear that

$$|\{(A,B)|A^n = B^2, A^n = -I\}| = |\{A|A^n = -I\}| * |\{B|B^2 = -I\}|.$$

Because n is odd, $-1 \in (\mathcal{F}_q - 0)^n$. By Proposition 2.2, there are $(q-1, n)$ many solutions for $x^n = -1$. Since we do not allow $x = -1$, there are $(q-1,n) - 1$ many solutions satisfying $A^n = -I$ and $A \neq \pm I$. We know $\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}$ and

$\begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix}$ are conjugate to each other. On the other hand for two representatives A and A' of Case 7, A' is conjugate to A if and only if $A' = A^{\pm}$. Up to conjugacy we get $\frac{(n,q-1)-1}{2}$ many solutions for $A^n = -I$, where $A = \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}$ for some x with $x \neq \pm 1$.

Fix A_1 to be $\begin{pmatrix} x_1 & 0 \\ 0 & x_1^{-1} \end{pmatrix}$ such that $x_1^n = -1$ and $x_1 \neq \pm 1$.

If $q \equiv 1 \pmod 4$, by Case 2, the set of collection of solutions for $A_1^n = B^2$ is $\mathcal{C}_{B_0}$ where $B_0 = \begin{pmatrix} x_0 & 0 \\ 0 & x_0^{-1} \end{pmatrix}$. Like in Case 5, we define an action Γ_{A_1} on Γ_{B_0}:$\Gamma_{A_1} \times \mathcal{C}_{B_0} \to \mathcal{C}_{B_0}$ by $(H, B) \to HBH^{-1}$. Let $N_{\Gamma_{A_1}}$ be the number of orbits.

Clearly $\Gamma_{A_1} = \Gamma_{B_0} = \Gamma_{B_0^{-1}}$. Then $|\Gamma_{A_1}(B_0)| = |\Gamma_{A_1}(B_0^{-1})| = |\Gamma_{A_1}/\Gamma_{A_1} \cap \Gamma_{B_0}| = 1$.

Given a $B = GB_0G^{-1}$, and $B \neq B_0^{\pm 1}$, By Proposition 2.11, B is not diagonal, $\Gamma_{A_1} \cap \Gamma_B = \{\pm I\}$. Therefore $|\Gamma_{A_1}(B)| = |\Gamma_{A_1}/\Gamma_{A_1} \cap \Gamma_B| = \frac{q-1}{2}$.

Hence

$$\frac{q-1}{2}(N_{\Gamma_{A_1}} - 2) + 2 = q(q+1).$$

We get $N_{\Gamma_{A_1}} = 2(q+3)$. Therefore up to conjugacy the number of solutions for $A_1^n = B^2$ is $2(q+3)$.

If $q \equiv 3 \pmod 4$, by case 2, the set of solutions for $A_1^n = B^2$ is $\mathcal{C}_{B_0'}$ where $B_0' = \begin{pmatrix} 0 & \sqrt{-\epsilon^{-1}} \\ \epsilon\sqrt{-\epsilon^{-1}} & 0 \end{pmatrix}$. By Table II, $\Gamma_A \cap \Gamma_{B_0'} = \{\pm I\}$. By the same argument of Case 5, up to conjugacy, the number of solution for $A_1^n = B^2$ is

$$\frac{|\mathcal{C}_{B_0}|}{|\Gamma_{A_1}/\Gamma_{A_1} \cap \Gamma_{B_0'}|} = \frac{q(q-1)}{(q-1)/2} = 2q.$$

Recall up to conjugacy the number of solutions for $A^n = -I$ is $\frac{(n,q-1)-1}{2}$, therefore the number of solutions for $A^n = B^2$ with $A^n = -1$ is

$$\begin{cases} ((n,q-1)-1)(q+3) & \text{if } q \equiv 1 \pmod 4, \\ ((n,q-1)-1)q & \text{if } q \equiv 3 \pmod 4). \end{cases}$$

7.b: If $x^n + 1 \neq 0$, then $b = c = 0$. Combining $a = dx^n$ and equation (3), we get $d^2x^n = 1$, which is equivalent to the equation $x^n = d^{-2}$. The number of solutions for $x^n = d^{-2}$ is equal to

$$\sum_{g \in G} |\{x | x^n = g\}| * |\{d | d^{-2} = g\}|,$$

where $G = (\mathcal{F}_q - 0)^2 \cap (\mathcal{F}_q - 0)^n$. Since $(n, 2) = 1$, $G = (\mathcal{F} - 0)^{2n}$. By Proposition 2.2, the number of solutions for $x^n = g$ and $(d^{-1})^2 = g$ with $g \in G$ are $(n, q-1)$ and $(n, 2)$ respectively. By Proposition 2.3, $|G| = \frac{q-1}{(q-1,2n)}$. Therefore we totally have $q - 1$ solutions for the equation $d^2x^n = 1$.

If $q \equiv 1 \pmod 4$, then $-1 \in (\mathcal{F}_q - 0)^2$. So we must throw the solutions of $x^n = d^{-2} = -1$ out. The number of solutions of $x^n = d^{-2} = -1$ is

$$|\{x|x^n = -1\}| * |\{d|d^{-2} = -1\}| = 2(n, q-1).$$

Obviously $1 \in (\mathcal{F}_q - 0)^2$. So we have to throw out 2 solutions out again. So the number of solutions is $q - 3 - 2(q-1, n)$ for $q \equiv 1 \pmod 4$.

If $q \equiv 3 \pmod 4$, then $-1 \notin (\mathcal{F}_q - 0)^2$. We just throw out 2 solutions if $q \equiv 3 \pmod 4$, that is to say the number of solutions is $q - 3$ for $q \equiv 3 \pmod 4$.

Clearly in this subcase both A and B are in the standard form of Case 7. Clearly (A, B) is not conjugate to $(A, -B)$. We know that if (A, B) is a solution, then (A^{-1}, B^{-1}) is a solution and conjugate to (A, B). On the other hand, (A, B) and (A', B') are conjugate to each other if and only if $A' = A^{\pm 1}$, in this situation $B' = B^{\pm 1}$. Therefore up to conjugacy, we have

$$\begin{cases} \frac{q-3}{2} - (n, q-1) & \text{if } q \equiv 1 \pmod 4, \\ \frac{q-3}{2} & \text{if } q \equiv 3 \pmod 4, \end{cases}$$

many solutions for $A^n \neq -I$ and $A^n = B^2$.

Add the number of solutions in case 7.a and case 7.b up, we get the number of solutions for the Equation (1) in case 7 is

$$\begin{cases} ((n, q-1) - 1)(q+3) + \frac{q-3}{2} - (n, q-1) & \text{if } q \equiv 1 \pmod 4, \\ ((n, q-1) - 1)q + \frac{q-3}{2} & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

Let $E(s) = \frac{1}{2}(1 + (-1)^s)$, $O(s) = \frac{1}{2}(1 - (-1)^s)$. As we know if $p \equiv 3 \pmod 4$, then $p^s \equiv 1 \pmod 4$ for s even, $p^s \equiv 3 \pmod 4$ for some s odd. The previous formula is equivalent to

$$\begin{cases} (n, p^s - 1) - 1)(p^s + 3) + \frac{p^s-3}{2} - (n, p^s - 1) & \text{if } p \equiv 1 \pmod 4, \\ ((n, p^s - 1) - 1)(p^s + 3E(s)) + \frac{p^s-3}{2} - E(s)(n, p^s - 1) & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Case 8. Let $A = \begin{pmatrix} x & y \\ \epsilon y & x \end{pmatrix}$, where $y \neq 0$. By Proposition 2.6, $A^n = \begin{pmatrix} u & v \\ \epsilon v & u \end{pmatrix}$ for some $u, v \in \mathcal{F}_q$. So Equation (1) is splitted into 3 subcases:(a) $A^n = I$, (b) $A^n = -I$, and (c) $A^n \neq \pm I$.

8.a: For $A^n = I$, we get

$$\{(A, B)|A^n = B^2, A^n = I\}| = |\{A|A^n = I\}| * |\{B|B^2 = I\}|.$$

By Case 1, we know $|\{B|B^2 = I\}| = 2$. By Proposition 2.2, the number of solutions of $A^n = I$ is equal to $(n, q+1)$. Since A is not allowed to be I, we throw one solution out. Clearly (A, I) and $(A, -I)$ are not conjugate to each other. On the other hand A is conjugate to A' in Ω if and only if $A' = A^{-1}$ for $A \in \Omega$. Hence we totally have $2\frac{(n,q+1)-1}{2} = (n, q+1) - 1$ solutions for the equation $A^n = B^2$ with $A^n = I$.

8.b: For $A^n = -I$. It is clear that

$$|\{(A, B)|A^n = B^2, A^n = -I\}| = |\{A|A^n = -I\}| * |\{B|B^2 = -I\}|.$$

First we count the solutions for the equation $A^n = -I$. By Proposition 2.2, the equation $A^n = -I$ has $(n, q+1)$ many solutions in the set Ω. We have to throw one solution out for $A \neq -I$. With the similar discussion of Case 8.a, up to conjugacy we have $\frac{(n,q+1)-1}{2}$ solutions for $A^n = -I$.

Fix A_1 to be $\begin{pmatrix} x_1 & y_1 \\ \epsilon y_1 & x_1 \end{pmatrix}$ such that $A_1^n = -I$ and $A_1 \neq I$.

If $q \equiv 1 \pmod 4$, then by Case 2, the set of collection of all solutions B is $\mathcal{C}_{B_0}$ where $B_0 = \begin{pmatrix} x_0 & 0 \\ 0 & x_0^{-1} \end{pmatrix}$ as we have defined as in Case 2. By Table II, $\Gamma_{A_1} \cap \Gamma_{B_0} = \{\pm I\}$. By the same argument of Case 5, the number of solutions for $A_1^n = B^2$ up to conjugacy is

$$\frac{|\mathcal{C}_{B_0}|}{|\Gamma_{A_1}/\Gamma_{A_1} \cap \Gamma_{B_0}|} = \frac{q(q+1)}{(q+1)/2} = 2q.$$

If $q \equiv 3 \pmod 4$, the set of collection of $A_1^n = B^2$ is $\mathcal{C}_{B_0'}$ where $B_0' = \begin{pmatrix} 0 & \sqrt{-\epsilon^{-1}} \\ \epsilon\sqrt{-\epsilon^{-1}} & 0 \end{pmatrix}$ as defined in Case 2. Clearly $\Gamma_{A_1} = \Gamma_{B_0'}$.

Similarly we define the action Γ_{A_1} on $\mathcal{C}_{B_0'}$:$\Gamma_{A_1} \times \mathcal{C}_{B_0'} \to \mathcal{C}_{B_0'}$ by $(H, B) \to HBH^{-1}$. We use $N_{\Gamma_{A_1}}$ to be the number of orbits.

Clearly $\Gamma_{A_1} = \Gamma_{B_0'} = \Gamma_{(B_0')^{-1}}$. Then $|\Gamma_{A_1}(B_0')| = |\Gamma_{A_1}((B_0')^{-1})| = |\Gamma_{A_1}/\Gamma_{A_1} \cap \Gamma_{B_0'}| = 1$.

Given a $B = GB_0G^{-1}$, and $B \neq B_0^{\pm 1}$. Then $B \notin \Omega$. By Proposition 2.12, $\Gamma_{A_1} \cap \Gamma_B = \{\pm I\}$. Therefore $|\Gamma_{A_1}(B)| = |\Gamma_{A_1}/\Gamma_{A_1} \cap \Gamma_B| = \frac{q+1}{2}$. Since $|\mathcal{C}_{B_0'}| = q(q-1)$, then

$$\frac{q+1}{2}(N_{\Gamma_{A_1}} - 2) + 2 = q(q-1).$$

We get $|\mathcal{C}_{B_0'}/\sim| = 2(q-1)$.

Since up to conjugacy the number of solutions for $A^n = -I$ is $\frac{(n,q+1)-1}{2}$, we get the number of solutions for $A^n = B^2$ with $A^n = -I$ is

$$\begin{cases} ((n,q+1)-1)q & \text{if } q \equiv 1 \pmod 4, \\ ((n,q+1)-1)(q-1) & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

8.c: For $A^n \neq \pm I$, let $A^n = \begin{pmatrix} u & v \\ \epsilon v & u \end{pmatrix}$ with some u, v and $v \neq 0$. By computation, $B^2 = \begin{pmatrix} a^2+bc & ab+bd \\ ac+dc & bc+d^2 \end{pmatrix}$. Hence Equation (1) becomes

$$\begin{pmatrix} u & v \\ \epsilon v & u \end{pmatrix} = \begin{pmatrix} a^2+bc & ab+bd \\ ac+dc & bc+d^2 \end{pmatrix}. \tag{11}$$

One has the equivalent relations

$$\begin{cases} u = a^2 + bc \\ v = ab + bd \\ \epsilon v = ac + bc \\ u = bc + d^2. \end{cases}$$

From $(a+d)b = v$ and $v \neq 0$, we get $a + d \neq 0$. From $u = a^2 + bc$ and $u = d^2 + bc$, we get $a^2 = d^2$. Therefore $a = d$. From $v = ab + bd$, $\epsilon v = ac + dc$ and $a = d$, we get $2ab\epsilon = 2ac$, i.e., $a(b\epsilon - c) = 0$. Since $a = d$ and $a + d \neq 0$, we get $c = \epsilon b$. This means $B \in \Omega$ too. So the problem is reduced to solve the equation $A^n = B^2$ in the group Ω. With the same discussion as we used in Case 7, we get $|\{(A,B)|A^n = B^2, A, B \in \Omega\}| = q + 1$. Since $A^n \neq I$, we must throw out $2(n, q+1)$ solutions. By Proposition 2.7. the square root of $-I$ is in Ω if and only if $q \equiv 3 \pmod 4$, By Proposition 2.7. In this condition, we throw $2(n, q+1)$ many solutions out again.

Clearly in this subcase both A and B are representatives of Case 8, then they have the same stabilizer. On the other hand, we know that if (A, B) is a solution, then (A^{-1}, B^{-1}) is a solution and conjugate to (A, B). we also know that in Case 8, (A, B) and (A', B') are conjugate to each other if and only if $A' = A^{\pm 1}$. So up to conjugacy the number of solutions for the equation $A^n = B^2$ with $A^n \neq \pm I$ are

$$\begin{cases} \frac{q+1}{2} - (n, q+1) & \text{if } q \equiv 1 \pmod 4, \\ \frac{q+1}{2} - 2(n, q+1) & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

Summarize above we totally have

$$\begin{cases} ((n, q+1) - 1)q + \frac{q+1}{2} - 1 & \text{if } q \equiv 1 \pmod 4, \\ ((n, q+1) - 1)(q - 1) + \frac{q+1}{2} - (n, q+1) - 1 & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

By the same discussion as in Case 7, the above is equivalent to

$$\begin{cases} ((n, p^s + 1) - 1)p^s + \frac{p^s - 1}{2} & \text{if } p \equiv 1 \pmod 4, \\ ((n, p^s + 1) - 1)(p^s - O(s)) + \frac{p^s - 1}{2} - O(s)(n, p^s + 1) & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Now we can give Table III for the number of solutions for each case which completes the proof of Theorem 1.1.

Table III

Case No.	**No. of Solutions Up To Conjugacy**
1.	2
2.	1
3.	2
4.	2
5.	$\begin{cases} q+1 & \text{if } q \equiv 1 \pmod 4 \text{ and } p \mid n, \\ q-1 & \text{if } q \equiv 3 \pmod 4 \text{ and } p \mid n, \\ 0 & \text{Otherwise.} \end{cases}$
6.	$\begin{cases} q+1 & \text{if } q \equiv 1 \pmod 4 \text{ and } p \mid n, \\ q-1 & \text{if } q \equiv 3 \pmod 4 \text{ and } p \mid n, \\ 0 & \text{Otherwise.} \end{cases}$
7.	$\begin{cases} ((n,q-1)-1)(q+2)+\frac{q-5}{2} & \text{if } q \equiv 1 \pmod 4, \\ ((n,q-1)-1)q+\frac{q-3}{2} & \text{if } q \equiv 3 \pmod 4. \end{cases}$
8.	$\begin{cases} ((n,q+1)-1)q+\frac{q-1}{2} & \text{if } q \equiv 1 \pmod 4, \\ ((n,q+1)-1)(q-2)+\frac{q-3}{2} & \text{if } q \equiv 3 \pmod 4. \end{cases}$

3. Counterexample for the result in [7]

In [7], the number of solutions of $A^n = B^2$ is computed case by case up to conjugacy. The following table is a result of [7].

Table IV

Case No.	No. of Solutions
1.	2
2.	$\begin{cases} q(q+1) & \text{if } q \equiv 1 \pmod 4, \\ q(q-1) & \text{if } q \equiv 3 \pmod 4 \end{cases}$
3.	2
4.	2
5.	$\begin{cases} \text{Case 2} & p \mid n \\ 0 & p \nmid n \end{cases}$
6.	$\begin{cases} \text{Case 2} & p \mid n \\ 0 & p \nmid n \end{cases}$
7.	$\begin{cases} \frac{(n,q-1)-1}{2}q(q+1) + \frac{q-3}{2} - (q-1,n) & \text{if } q \equiv 1 \pmod 4, \\ \frac{(n,q-1)-1}{2}q(q-1) + \frac{q-3}{2} & \text{if } q \equiv 3 \pmod 4. \end{cases}$
8.	$\frac{q+1}{2} - 1 - \frac{1}{2}(1 + (-1)^{\frac{q-1}{2}})$.

The table IV of [7] is completely different from our Table III except Case 1, Case 3 and Case 4. The main difference is in the result of Case 8. The formula given in [7] in Case 8 is $\frac{q+1}{2} - 1 - \frac{1}{2}(1 + (-1)^{\frac{q-1}{2}})$. While in this paper, by our computation, the number of solutions of the same case is

$$\begin{cases} ((n,q+1)-1)q + \frac{q-1}{2} & \text{if } q \equiv 1 \pmod 4, \\ ((n,q-1)-1)(q-1) + \frac{q-1}{2} - (n,q+1) & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

They are not equivalent to each other. There is an error in [7] by the following examples.

Example 1. Let $q = 5, n = 3$. Then $\mathcal{F}_q = \{0,1,2,3,4\}$. Since $\sqrt{2} \notin \mathcal{F}_q$, we choose $\epsilon = 2$. Write $A = \begin{pmatrix} a & b \\ \epsilon b & a \end{pmatrix}$ as the pair (a,b), where $a, b \in \mathcal{F}_q$ and $a^2 - \epsilon b^2 = 1$. If $\begin{pmatrix} u & v \\ \epsilon v & u \end{pmatrix} = \begin{pmatrix} a & b \\ \epsilon b & a \end{pmatrix}^n$, we write $(u,v) = (a,b)^n$. Let $\Omega = \{(a,b) | a^2 - \epsilon b^2 = 1 \text{ in } \mathcal{F}_q\}$. We determine a by $a^2 = 1 + \epsilon b^2$. Thus

$$\Omega = \{(1,0),(4,0),(2,2),(2,3),(3,2),(3,3)\}.$$

Let $\Omega^2 = \{(u,v)|(u,v) = (a,b)^2 \text{ for some } (a,b) \in \Omega\}$, . Clearly if $(u,v) = (a,b)^2$, then $u = a^2 + \epsilon b^2$, $v = 2ab$. Thus

$$\Omega^2 = \{(1,0),(2,2),(2,3)\}.$$

Let $\Omega^3 = \{(u,v)|(u,v) = (a,b)^3 \text{ for some } (a,b) \in \Omega\}$. Obviously if $(u,v) = (a,b)^3$, then $u = a^3 + 3ab^2\epsilon$, $v = 3a^2b + b^3\epsilon$. Thus

$$\Omega^3 = \{(1,0),(-1,0)\}.$$

So for any $A \in \Omega$, $A^3 = \pm I$. The number of solutions of both $A^3 = B^2$ with $A \in \Omega - \{\pm I\}$ is equal to

$$|\{B|B^2 = I\}| * |\{A|A^3 = I, A \in \Omega_1\}| + |\{B|B^2 = -I\}| * |\{A|A^3 = -I, A \in \Omega_1\}|.$$

By computation, $\{(a,b)|(a,b)^3 = I\} = \{(1,0),(2,3),(2,2)\}$. The solutions for $B^2 = I$ is $\pm I$. Since $(2,3)^{-1} = (2,2)$, the matrix $(2,3)$ are conjugate to the matrix $(2,2)$, so up to conjugacy we have 2 pairs solutions for $A^3 = B^2 = I$ in Case 8:

$$1. A = \begin{pmatrix} 2 & 3 \\ \epsilon 3 & 2 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

$$2. A = \begin{pmatrix} 2 & 3 \\ \epsilon 3 & 2 \end{pmatrix}, B = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

We also get $\{(a,b)|(a,b)^3 = -I\} = \{(-1,0),(3,2),(3,3)\}$. Up to conjugacy we only have one solution $A = (3,2)$ for $A^3 = -I$ in Case 8. We list the solution of $B^2 = -I$ below, where the matrices in the same row are the orbits under the action of $\Gamma_{(3,2)}$.

1. $\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 4 & 4 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 1 \\ 3 & 1 \end{pmatrix},$

2. $\begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 2 & 4 \end{pmatrix},$

3. $\begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix},$

4. $\begin{pmatrix} 3 & 0 \\ 4 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 4 & 3 \end{pmatrix}, \begin{pmatrix} 0 & 3 \\ 3 & 0 \end{pmatrix},$

5. $\begin{pmatrix} 2 & 0 \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 1 & 4 \end{pmatrix},$

6. $\begin{pmatrix} 3 & 0 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 3 & 4 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 2 \\ 4 & 1 \end{pmatrix},$

7. $\begin{pmatrix} 2 & 0 \\ 3 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 4 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 4 \\ 0 & 3 \end{pmatrix},$

8. $\begin{pmatrix} 3 & 0 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 3 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 1 \\ 0 & 2 \end{pmatrix},$

9. $\begin{pmatrix} 2 & 2 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 4 \\ 1 & 0 \end{pmatrix},$

10. $\begin{pmatrix} 3 & 3 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 4 & 0 \end{pmatrix}$.

Therefore up to conjugacy we have 12 solutions for $A^3 = B^2$ in Case 8.

By the formula given in [7], the number of solutions is

$$\frac{q+1}{2} - 1 - \frac{1}{2}(1 + (-1)^{\frac{q-1}{2}}) = \frac{5+1}{2} - 1 - \frac{1}{2}(1 + (-1)^{\frac{5-1}{2}}) = 1.$$

By the formula given in table II, the number of solutions is

$$((n, q+1) - 1)q + \frac{q-1}{2} = ((3, 5+1) - 1)5 + \frac{5-1}{2} - 1 = 12.$$

Example 2. Let $q = 7, n = 3$. By simple calculation, $\sqrt{3} \notin \mathcal{F}_7$, let $\epsilon = 3$. Then

$$\Omega = \{(1,0), (6,0), (2,1), (2,6), (0,3), (0,4), (5,1), (5,6)\},$$

$$\Omega^2 = \{(1,0), (6,0), (0,3), (0,4)\},$$

$$\Omega^3 = \Omega.$$

Clearly there is no matrix $A \in \Omega_1$ satisfying $A^3 = \pm I$. So

$$\{(A, B)|A^3 = B^2, A \in \Omega_1\} = \{(A, B)|A^3 = B^2, A, B \in \Omega_1\},$$

which is listed below

$$\{((2,1), (0,3)), ((2,6), (0,4)), ((5,1), (0,4)), ((5,6), (0,3))\}.$$

Clearly $((2,1),(0,3))$ and $((2,6),(0,4))$ are conjugate to each other, and $((5,1),(0,4))$ and $((5,6),(0,3))$ are conjugate to each other. Up to the conjuagacy, the number of solutions is 2. By the formula given by [7], the number of solutions is

$$\frac{q+1}{2} - 1 - \frac{1}{2}(1 + (-1)^{\frac{q-1}{2}}) = 5.$$

By the formula given in table II, up the conjugacy the number of solutions is

$$((n, q+1) - 1)(q-1) + \frac{q-1}{2} - (n, q+1) = ((3,8) - 1)(7-1) + \frac{7-1}{2} - (3,8) = 2.$$

4. Finding the Zeta function

What we are going to do now is to use the previous information on the counting of the representations to evaluate the Zeta function of a torus knot. First we give the definition.

Definition 4.1. Let K be a Torus knot in 3-space. Fix a prime number p. Let N_s be the number of representations of the knot group into $SL(\mathcal{F}_{p^s})$, up to conjugacy. The the Zeta function is simply the formal power series

$$Z(p, T) = \exp\left(\sum_{s=1}^{\infty} \frac{N_s T^s}{s}\right) \tag{12}$$

We will keep p fixed, once and for all. Now notice that if N_s^i is the number of solution that come from Case i above then: $N_s = \sum_{i=1}^{8} N_s^i$,

$$\begin{aligned} Z(p,T) &= \exp(\sum_{s=1}^{\infty} \frac{N_s T^s}{s} = \exp(\sum_{s=1}^{\infty}\sum_{i} \frac{N_s^i T^s}{s}) \\ &= \prod_i \exp(\sum_{s=1}^{\infty} \frac{N_s^i T^s}{s}) = \prod_i Z_i, \end{aligned}$$

where $Z_i = \exp(\sum_{s=1}^{\infty} \frac{N_s^i T^s}{s})$, so basically we can just find the Zeta function for each individual case, then multiply the answers together when all done.

Case 1. Recall that in this situation we have 2 solutions, no matter what $q = p^s$ was. So we can say $N_s^1 = 2$, so

$$\begin{aligned} Z_1 &= \exp(\sum_{s=1}^{\infty} \frac{N_s^1 T^s}{s}) = \exp(\sum_{s=1}^{\infty} 2\frac{T^s}{s}) \\ &= \exp(2\sum_{s=1}^{\infty} \frac{T^s}{s}) = \exp(-2\log(1-T)) \\ &= \frac{1}{(1-T)^2}. \end{aligned}$$

Case 2. From table III, we have 1 solution up to conjugacy. So

$$Z_2 = \frac{1}{1-T}$$

Similarly we get

$$Z_3 = \frac{1}{(1-T)^2},$$

$$Z_4 = \frac{1}{(1-T)^2},$$

Case 5. From table III, we have no solution if $p \nmid n$. If $p \mid n$, the number of solutions is equal to

$$\begin{cases} q+1 & \text{if } q \equiv 1 \pmod 4, \\ q-1 & \text{if } q \equiv 3 \pmod 4, \end{cases}$$

If $p \equiv 1 \pmod 4$, then $p^s \equiv 1 \pmod 4$ for all s. If $p \equiv 3 \pmod 4$, then $p^s \equiv 3 \pmod 4$ for s is odd, $p^s \equiv 1 \pmod 4$ for s is even. Therefore the previous formula is equivalent to

$$\begin{cases} p^s + 1 & \text{if } p \equiv 1 \pmod 4, \\ p^s + (-1)^s & \text{if } p \equiv 3. \pmod 4. \end{cases}$$

Therefore for $p \equiv 1 \pmod 4$ and $p \mid n$, we get

$$\begin{aligned} Z_5 &= \exp(\sum_{s=1}^{\infty} \frac{N_s^5 T^s}{s}) \\ &= \exp(\sum_{s=1}^{\infty} \frac{(1+p^s)T^s}{s}) \\ &= \frac{1}{(1-pT)(1-T)}. \end{aligned}$$

For $p \equiv 3 \pmod 4$ and $p \mid n$, we get

$$\begin{aligned} Z_5 &= \exp(\sum_{s=1}^{\infty} \frac{N_s^5 T^s}{s}) \\ &= \exp(\sum_{s=1}^{\infty} \frac{(p^s+(-1)^s)T^s}{s}) \\ &= \frac{1}{(1-pT)(1+T)}. \end{aligned}$$

In general,

$$Z_5 = \begin{cases} 1 & \text{if } p \nmid n, \\ \frac{1}{(1-pT)(1+(-1)^{\frac{p+1}{2}}T)} & \text{if } p \mid n. \end{cases}$$

Similarly

$$Z_6 = \begin{cases} 1 & \text{if } p \nmid n, \\ \frac{1}{(1-pT)(1+(-1)^{\frac{p+1}{2}}T)} & \text{if } p \mid n. \end{cases}$$

To calculate Z_7, we need to deal with $\sum(p^s-1,n)\frac{T^s}{s}$. So we first discuss how to calculate $\sum_{s=1}^{\infty}((p^s-1,n)-1)\frac{T^s}{s}$. By Fermat's little Theorem, for each $d|n$, there exists a $\psi(d)$, such that $p^{\psi(d)} \equiv 1 \pmod d$ if $(d,p)=1$. Clearly if $(n,p) \neq 1$, then $(n,p^s-1)=1$ for all s. In this situation, we obtain

$$Z_7 = \begin{cases} \sqrt{\frac{(1-T)^5}{1-pT}} & \text{if } p \equiv 1 \pmod 4 \\ \sqrt{\frac{(1-T)^4(1+T)^2}{1-pT}} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Suppose $(n,p)=1$.

Given a natural number p, we can write $n = p_1^{t_1}p_2^{t_2}\dots p_r^{t_r}$ for some distinguish prime number p_i. So we calculate three different cases i)$n=p_1$, ii)$n=p_1^2$, iii)$n=p_1p_2$ where p_1,p_2 are different prime number, with $p_1,p_2>2$. Then the other cases can be computed by the same algorithm. Write $F(s)=\sum_{s=1}^{\infty}((p^s-1,p_1)-1)\frac{T^s}{s}$.

i: Let $n = p_1$. Let m_1 be the smallest positive integer satisfying $p^s \equiv 1 \pmod{p_1}$. If $p^m \equiv 1 \pmod{p_1}$, we can write $m = km_1$ for some integer k. Therefore

$$
\begin{aligned}
F(s) &= \sum_{s=1}^{\infty}(((p^s-1,p_1)-1)\frac{T^s}{s} \\
&= (p_1-1)\sum_{k=1}^{\infty}\frac{T^{m_1k}}{m_1k} \\
&= -\frac{p_1-1}{m_1}\ln(1-T^{m_1}).
\end{aligned}
$$

ii: Let $n = p_1^2$. Let m_1 as above. Let m_2 be the smallest positive integer satisfying $p^s \equiv 1 \pmod{p_1^2}$. Clearly $m_1|m_2$. Therefore

$$
\begin{aligned}
F(s) &= \sum_{s=1}^{\infty}(((p^s-1,p_1^2)-1)\frac{T^s}{s} \\
&= (p_1-1)\sum_{k=1}^{\infty}\frac{T^{m_1k}}{m_1k} - (p_1-1)\sum_{k=1}^{\infty}\frac{T^{m_2k}}{m_2k} + (p_1^2-1)\sum_{k=1}^{\infty}\frac{T^{m_2k}}{m_2k} \\
&= -\frac{p_1-1}{m_1}\ln(1-T^{m_1}) + \frac{p_1-1}{m_2}\ln(1-T^{m_2}) - \frac{p_1^2-1}{m_2}\ln(1-T^{m_2}) \\
&= -\frac{p_1-1}{m_1}\ln(1-T^{m_1}) - \frac{p_1(p_1-1)}{m_2}\ln(1-T^{m_2}).
\end{aligned}
$$

iii: For $n = p_1p_2$. Choose m_1 as above. Let m_3, m_4 be the smallest positive integers satisfying $p^s \equiv 1 \pmod{p_2}$ and $p^s \equiv 1 \pmod{p_1p_2}$ respectively. Clearly $m_1 \mid m_4$ and $m_3 \mid m_4$. Then

$$
\begin{aligned}
F(s) =& \sum_{s=1}^{\infty}(((p^s-1,p_1p_2)-1)\frac{T^s}{s} \\
=& (p_1-1)\sum_{k=1}^{\infty}\frac{T^{m_1k}}{m_1k} - (p_1-1)\sum\frac{T^{m_4k}}{m_4k} + (p_2-1)\sum_{k=1}^{\infty}\frac{T^{m_3k}}{m_3k} \\
&- (p_2-1)\sum_{k=1}^{\infty}\frac{T^{m_4k}}{m_4k} + (p_1p_2-1)\sum_{k=1}^{\infty}\frac{T^{m_4k}}{m_4k} \\
=& -\frac{p_1-1}{m_1}\ln(1-T^{m_1}) + \frac{p_1-1}{m_4}\ln(1-T^{m_4}) \\
&- \frac{p_3-1}{m_3}\ln(1-T^{m_3}) + \frac{p_2-1}{m_4}\ln(1-T^{m_4}) - \frac{p_1p_2-1}{m_4}\ln(1-T^{m_4}) \\
=& -\frac{p_1-1}{m_1}\ln(1-T^{m_1}) - \frac{p_2-1}{m_3}\ln(1-T^{m_3}) - \frac{(p_1-1)(p_2-1)}{m_4}\ln(1-T^{m_4}).
\end{aligned}
$$

To simplify the formula, let $f(p_1) = \frac{p_1-1}{m_1}$, $f(p_2) = \frac{p_1(p_1-1)}{m_2}$, and $f(p_1p_2) = \frac{(p_1-1)(p_2-1)}{m_3}$. So for $n = p_1$, we get,

$$
Z_7 = \begin{cases}
\frac{1}{(1-p^{m_1}T^{m_1})^{f(p_1)}(1-T^{m_1})^{2f(p_1)}} \\
*\frac{\sqrt{(1-T)^5}}{\sqrt{1-pT}}, & p \equiv 1 \pmod 4, \\
\\
\frac{1}{(1-(pT)^{m_1})^{f(p_1)}} * \frac{1}{(1-T^{m_1})^{f(p_1)}} * \frac{1}{(1-(-T)^{m_1})^{f(p_1)}} \\
*\sqrt{\frac{(1-T)^4(1+T)}{1-pT}}, & p \equiv 3 \pmod 4.
\end{cases}
$$

For $n = p_1^2$, we get

$$
Z_7 = \begin{cases}
\frac{1}{(1-p^{m_1}T^{m_1})^{f(p_1)}(1-T^{m_1})^{2f(p_1)}} \frac{1}{(1-p^{m_2}T^{m_2})^{f(p_1^2)}} \\
\frac{1}{(1-T^{m_2})^{2f(p_1^2)}} * \frac{\sqrt{(1-T)^5}}{\sqrt{1-pT}} & \text{if } p \equiv 1 \pmod 4, \\
\\
\frac{1}{(1-(pT)^{m_1})^{f(p_1)}} * \frac{1}{(1-T^{m_1})^{f(p_1)}} * \frac{1}{(1-(-T)^{m_1})^{f(p_1)}} \\
\frac{1}{(1-(pT)^{m_2})^{f(p_1^2)}} * \frac{1}{(1-T^{m_1})^{f(p_1^2)}} * \frac{1}{(1-(-T)^{m_2})^{f(p_1^2)}} \\
\sqrt{\frac{(1-T)^4(1+T)}{1-pT}} & \text{if } p \equiv 3 \pmod 4.
\end{cases}
$$

For $n = p_1p_2$, we get

$$
Z_7 = \begin{cases}
\frac{1}{(1-p^{m_1}T^{m_1})^{f(p_1)}(1-T^{m_1})^{2f(p_1)}} \frac{1}{(1-p^{m_3}T^{m_3})^{f(p_2)}} \\
\frac{1}{(1-T^{m_3})^{2f(p_3)}} * \frac{1}{(1-p^{m_4}T^{m_4})^{f(p_3)}(1-T^{m_4})^{2f(p_3)}} \\
\frac{\sqrt{(1-T)^5}}{\sqrt{1-pT}} & \text{if } p \equiv 1 \pmod 4, \\
\\
\frac{1}{(1-(pT)^{m_1})^{f(p_1)}} * \frac{1}{(1-T^{m_1})^{f(p_1)}} * \frac{1}{(1-(-T)^{m_1})^{f(p_1)}} \\
\frac{1}{(1-(pT)^{m_3})^{f(p_2)}} * \frac{1}{(1-T^{m_3})^{f(p_2)}} * \frac{1}{(1-(-T)^{m_3})^{f(p_2)}} \\
\frac{1}{(1-(pT)^{m_4})^{f(p_1p_2)}} * \frac{1}{(1-T^{m_4})^{f(p_1p_2)}} * \frac{1}{(1-(-T)^{m_4})^{f(p_1p_2)}} \\
\sqrt{\frac{(1-T)^4(1+T)}{1-pT}} & \text{if } p \equiv 3 \pmod 4.
\end{cases}
$$

To compute the Zeta function of case 8, we use the same method as we have shown in the computation of Zeta function of Case 7. And by the same reason as above, we only give the Zeta function for i)$n = p_1$, ii)$n = p_1^2$, iii)$n = p_1p_2$ for some p_1, p_2 are prime number with $p_1, p_2 > 2$ and $p_1 \neq p_2$. To simplify the discussion, we always suppose there is a solution for the equation $p^s \equiv -1 \pmod n$.

i)For $n = p_1$. Let m'_1 be the smallest positive solution for $p^s \equiv -1 \pmod{p}_1$. By Proposition 4.1, we get if $p^m \equiv -1 \pmod{p_1}$, then $m = (2k+1)m_1$ for some integer $k \geq 0$. Clearly $m_1 = 2m'_1$. We compute the subcase of $p \equiv 1 \pmod 4$. So

$$N_8^s = ((p_1, p^s + 1) - 1)p^s + \frac{p^s - 1}{2}$$

We compute $\ln Z_8$ first.

$$\begin{aligned}
\ln(Z_8) &= \sum_{s=1}^{\infty}(((n, p^s+1) - 1)p^s + \frac{p^s - 1}{2})\frac{T^s}{s} \\
&= \frac{p_1 - 1}{m_1}\sum_{k=1}^{\infty}\frac{(pT)^{(2k+1)m'_1}}{2k+1} + \frac{1}{2}\sum_{s=1}^{\infty}\frac{p^sT^s - T^s}{s} \\
&= \frac{p_1 - 1}{2m'_1}\ln\frac{1+(pT)^{m'_1}}{1-(pT)^{m'_1}} + \frac{1}{2}\ln\frac{1-T}{1-pT} \\
&= f(p_1)\ln(\frac{1+(pT)^{\frac{m_1}{2}}}{1-(pT)^{\frac{m_1}{2}}}) + \frac{1}{2}\ln(\frac{1-T}{1-pT}).
\end{aligned}$$

$$Z_8 = (\frac{1+(pT)^{m'_1}}{1-(pT)^{m'_1}})^{f(p_1)}\sqrt{\frac{1-T}{1-pT}}.$$

In general we get

$$\begin{cases}
(\frac{1+(pT)^{m'_1}}{1-(pT)^{m'_1}})^{f(p_1)}\sqrt{\frac{1-T}{1-pT}} & \text{if } p \equiv 1 \pmod 4, \\
(\frac{1+(pT)^{m'_1}}{1-(pT)^{m'_1}})^{f(p_1)}(\frac{1-T^{m'_1}}{1+T^{m'_1}})^{f(p_1)} & \\
*(\frac{1+(-T)^{m'_1}}{1-(-T)^{m'_1}})^{f(p_1)}\sqrt{\frac{(1-T)^2}{(1-pT)(1+T)}} & \text{if } p \equiv 3 \pmod 4.
\end{cases}$$

ii)For $n = p_1^2$. Choose m'_1 as above, let m'_2 be the smallest positive solution for $p^s \equiv -1 \pmod{p_1^2}$. Clearly $m_1 | m_2$. And $m_2 = 2m'_2$. By the similarly discussion as above, we get Z_8 equal to

$$\begin{cases}
(\frac{1+(pT)^{m'_1}}{1-(pT)^{m'_1}})^{f(p_1)}(\frac{1+(pT)^{m'_2}}{1-(pT)^{m'_2}})^{f(p_1^2)}\sqrt{\frac{1-T}{1-pT}} & \text{if } p \equiv 1 \pmod 4, \\
(\frac{1+(pT)^{m'_1}}{1-(pT)^{m'_1}})^{f(p_1)}(\frac{1-T^{m'_1}}{1+T^{m'_1}})^{f(p_1)}(\frac{1+(-T)^{m'_1}}{1-(-T)^{m'_1}})^{f(p_1)} & \\
(\frac{1+(pT)^{m'_2}}{1-(pT)^{m'_2}})^{f(p_1^2)}(\frac{1-T^{m'_2}}{1+T^{m'_2}})^{f(p_1^2)}(\frac{1+(-T)^{m'_2}}{1-(-T)^{m'_2}})^{f(p_1^2)}\sqrt{\frac{(1-T)^2}{(1-pT)(1+T)}} & \text{if } p \equiv 3 \pmod 4.
\end{cases}$$

iii)For $n = p_1p_2$. Choose m'_1 as above, let m'_3 be the smallest positive solution for $p^s \equiv -1 \pmod{p}_2$, m'_4 be the smallest positive solution for $p^s \equiv -1 \pmod{p_1p_2}$. Clearly $m'_1 | m'_4$, $m'_3 | m'_4$, and m'_1, m'_3 are coprime. We also get $m_3 = 2m'_3$ and $m_4 = m'_4$. Therefore Z_8 equal to

$$\begin{cases} (\frac{1+(pT)^{m'_1}}{1-(pT)^{m'_1}})^{f(p_1)}(\frac{1+(pT)^{m'_3}}{1-(pT)^{m'_3}})^{f(p_3)} \\ *(\frac{1+(pT)^{m'_4}}{1-(pT)^{m'_4}})^{f(p_1p_2)}\sqrt{\frac{1-T}{1-pT}} & \text{if } p\equiv 1 \pmod 4, \\ \\ (\frac{1+(pT)^{m'_1}}{1-(pT)^{m'_1}})^{f(p_1)}(\frac{1-T^{m'_1}}{1+T^{m'_1}})^{f(p_1)}(\frac{1+(-T)^{m'_1}}{1-(-T)^{m'_1}})^{f(p_1)} \\ *(\frac{1+(pT)^{m'_3}}{1-(pT)^{m'_3}})^{f(p_2)}(\frac{1-T^{m'_3}}{1+T^{m'_3}})^{f(p_2)}(\frac{1+(-T)^{m'_3}}{1-(-T)^{m'_2}})^{f(p_2)} \\ (\frac{1+(pT)^{m'_4}}{1-(pT)^{m'_4}})^{f(p_1p_2)}(\frac{1-T^{m'_4}}{1+T^{m'_4}})^{f(p_1p_2)}(\frac{1+(-T)^{m'_4}}{1-(-T)^{m'_4}}^{f(p_1p_2)}\sqrt{\frac{(1-T)^2}{(1-pT)(1+T)}} & \text{if } p\equiv 3 \pmod 4. \end{cases}$$

In [7], a modified Zeta-function of a knot is defined as

$$\lambda_K(p,T)=\exp(\sum_{s=1}^{\infty}(\frac{N'_sT^s}{s})), \tag{13}$$

where N'_s is the number of non-diagonal representations of the fundamental group of the torus knot into $SL(\mathcal{F}_{p^s})$, counted up to conjugacy.

Let $p\equiv 1 \pmod 4$. We show that for $n=p_1$, $\lambda_K^{-2}(p,T)$ is a polynomial. Here we have two subcases 1) $p\nmid n$. 2)$p\mid n$. Denote $\exp(\sum\frac{(N_s^i)'T^s}{s})$ by λ_i where $(N_s^i)'$ is the number of non-diagonal representations in Case i.

1) Let $p\nmid n$.

i: Both representative is Case 1 are diagonal, so

$$\lambda_1=1$$

ii: Both representative is Case 2 are diagonal, so

$$\lambda_2=1$$

iii: Obviously no diagonal representations since A is not diagonal. So $\lambda_3=\frac{1}{(1-T)^2}$.

iv: Obviously no diagonal representations since A is not diagonal. So $\lambda_4=\frac{1}{(1-T)^2}$.

v: By table III, we get $N_5^s=0$, so $\lambda_5=1$.

vi: By table III, we get $N_6^s=0$, so $\lambda_6=1$.

vii: The representations of subcase 7.b are diagonal. In subcase 7.a, for the solution (A,B), it is diagonal if and only if B is diagonal. For each fixed A_1, there are two diagonal solutions satisfying $A_1^n=B^2$. So $(N_s^7)'=\frac{1}{2}((n,p^s-1)-1)(2(p^s+3)-2)=((n,p^s-1)-1)(p^s+2)$. We get

$$\lambda_7=\frac{1}{(1-p^{m_1}T^{m_1})^{f(p_1)}(1-T^{m_1})^{2f(p_1)}}.$$

viii: Obviously all the presentations in Case 8 are not diagonal. So

$$\lambda_8=\frac{1+(pT)^{m'_1}}{1-(pT)^{m'_1}})^{f(p_1)}\sqrt{\frac{1-T}{1-pT}}.$$

Therefore

$$\lambda^2 = 1 * 1 * \frac{1}{(1-T)^4} * \frac{1}{(1-T)^4} * 1 * 1$$
$$* \frac{1}{(1-p^{m_1}T^{m_1})^{2f(p_1)}(1-T^{m_1})^{4f(p_1)}} * (\frac{1+(pT)^{m'_1}}{1-(pT)^{m'_1}})^{2f(p_1)} \frac{1-T}{1-pT}$$
$$= \frac{1}{(1-T)^7} \frac{1}{((1-(pT)^{m'_1})^{4f(p_1)}(1-T^{m_1})^{4f(p_1)}} \frac{1}{1-pT}.$$

Hence λ^{-2} is a polynomial.

2)Let $p \mid n$.

i: Both representative is Case 1 are diagonal, so

$$\lambda_1 = 1$$

ii: Both representative is Case 2 are diagonal, so

$$\lambda_2 = 1$$

iii: Obviously no diagonal representations since A is not diagonal. So $\lambda_3 = \frac{1}{(1-T)^2}$.
iv: Obviously no diagonal representations since A is not diagonal. So $\lambda_4 = \frac{1}{(1-T)^2}$.
v: Clearly no diagonal representations since A is not diagonal, So $\lambda_5 = \frac{1}{(1-pT)(1-T)}$.
vi: Clearly no diagonal representations since A is not diagonal. So $\lambda_6 = \frac{1}{(1-pT)(1-T)}$.
vii: The representations of subcase 7.b are diagonal. In subcase 7.a, since $p \mid n$, $(n, p^s - 1) - 1 = 0$, we get

$$\lambda_7 = 1.$$

viii: Obviously all the presentations in Case 8 are not diagonal. So

$$\lambda_8 = \sqrt{\frac{1-T}{1-pT}}.$$

Therefore

$$\lambda^2 = 1 * 1 * \frac{1}{(1-T)^4} \frac{1}{(1-T)^4} \frac{1}{(1-pT)^2(1-T)^2}$$
$$\frac{1}{(1-pT)^2(1-T)^2} * 1 * \frac{1-T}{1-pT}$$
$$= \frac{1}{(1-T)^{11}(1-pT)^5}.$$

Clearly λ^{-2} is a polynomial.

Let $n = p_1^2$. Then

$$\lambda^2 = \frac{1}{(1-T)^4}\frac{1}{(1-T)^4} * \frac{1}{(1-p^{m_1}T^{m_1})^{2f(p_1)}(1-T^{m_1})^{4f(p_1)}}\frac{1}{(1-p^{m_2}T^{m_2})^{2f(p_1^2)}}$$

$$* \frac{1}{(1-T^{m_2})^{4f(p_1^2)}}(\frac{1+(pT)^{m_1'}}{1-(pT)^{m_1'}})^{2f(p_1)}(\frac{1+(pT)^{m_2'}}{1-(pT)^{m_2'}})^{2f(p_1^2)}\frac{1-T}{1-pT}$$

$$= \frac{1}{(1-T)^7}\frac{1}{((1-(pT)^{m_1'})^{4f(p_1)}(1-T^{m_1})^{4f(p_1)}}\frac{1}{((1-(pT)^{m_2'})^{4f(p_1^2)}(1-T^{m_2})^{4f(p_1^2)}}$$

$$* \frac{1}{1-pT}.$$

Clearly λ^{-2} is a polynomial.

Let $n = p_1p_2$. Then

$$\lambda^2 = \frac{1}{(1-T)^7}\frac{1}{((1-(pT)^{m_1'})^{4f(p_1)}(1-T^{m_1})^{4f(p_1)}}\frac{1}{((1-(pT)^{m_3'})^{4f(p_2}(1-T^{m_3})^{4f(p_2)}}$$

$$* \frac{1}{((1-(pT)^{m_4'})^{4f(p_1p_2)}(1-T^{m_4})^{4f(p_1p_2)}} * \frac{1}{1-pT}.$$

Obviously λ^{-2} is a polynomial.

REFERENCES

[1] S. Akbulut, J. MaCarthy, Casson's invariant for oriented homology 3-spheres, an exposition, Math. Notes **36**, (1990).

[2] W. Fulton and J. Harris, *Representation Theory: a first course*, Springer-Verlag, (1950).

[3] W. Li, *Casson-Lin's invariant and Floer homology*, J. Knot Theory and its Ramifications, Vol **6**, No.6 (1997), 851-877.

[4] W. Li, *Knot and Link Invariants and Moduli Spaces of Parabolic Bundles*, to appear in Communications in Contemporary Mathematics.

[5] X. S. Lin, *A knot invariant via representation spaces*, J. Diff. Geom., **35**, 337 - 357 (1992).

[6] Kenneth H. Rosen, *Elementary Number Theory And Its Applications*,Addison-Wesley, (2000).

[7] Jeffery M. Sink, *A Zeta-Function For A Knot Using $SL_2(\mathcal{F}_{p^s})$ Representations*, Knots in Hellas' 98, Proceedings of The International Conference on Knot Theory and Its Ramification, 452-470.

VITA

Liang Xu

Candidate for the Degree of

Master of Science

Thesis: $SL_2(\mathcal{F}q)$---REPRESENTATIONS OF TORUS KNOTS

Major Field: Mathematics

Biographical:

Education: Received Bachelor of Science degree in Mathematics in Hubei University, Wuhan, Hubei, China in July, 1995. Attended Graduate School in Wuhan University after that. Completed the requirements for the Master of Science degree with a major in Pure Mathematics at Oklahoma State University in August 2001.

Experience: Employed by Wuhan University, Department of Mathematics as a graduate teaching assistant from 1997-1998; employed by Central China Normal University, Department of Mathematics as a lecturer from 1998-1999; employed by Oklahoma State University, Department of Mathematics as a graduate teaching assistant from 2000 to 2001.