

Jan. 10th, 2012 in KAIST

$SL(2, \mathbb{Z}/d)$ -representations of a knot group and
Alexander polynomial as an obstruction

北野 晃朗 (KITANO Teruaki) (Soka Univ.)

目次

1	Introduction	2
2	Theorem of de Rham	9
3	Construction of a homomorphism of $G(K)$ into symmetric groups	18
4	Example: Trefoil knot	25
5	$SL(2, \mathbb{Z}/d)$ -representation of $G(K)$	31
6	$GL(2, \mathbb{Z}/p)$ -representation of $G(K)$	34

1 Introduction

we fix some notations in this talk:

- K : a knot in S^3 .
- $G(K) = \pi_1(S^3 - K)$: its knot group.
- $G(K) = \langle x_1, \dots, x_n \mid r_1, \dots, r_n \rangle$: Wirtinger presentation.
- $\alpha : G(K) \rightarrow \mathbb{Z} = \langle t \rangle$: the abelianization of $G(K)$.
- $\alpha_* : \mathbb{Z}G(K) \rightarrow \mathbb{Z}\langle t \rangle = \mathbb{Z}[t, t^{-1}]$: induced map on the integral group ring.
- $A \in M((n-1) \times n; \mathbb{Z}[t, t^{-1}])$: Alexander matrix of $G(K)$ defined by the presentation.
- $A(a) = A|_{t=a} \in M((n-1) \times n; \mathbb{Z}[t, t^{-1}])$: the matrix obtained by substituting $t = a$ to A .
- \mathfrak{S}_d : the symmetric group of degree d .

In this talk we suppose

- any presentation of $G(K)$ is a **Wirtinger presentation**.

By applying Fox's free differentials to the relators of $G(K)$, **Alexander matrix** is defined by

$$A = \left(\alpha_* \left(\frac{\partial}{\partial x_j} (r_i) \right)_{ij} \right)$$

and the Alexander polynomial $\Delta_K(t)$ is defined to be a $(n - 1)$ -minor.

Here after changing a presentation if we need, we can assume that some $(n - 1)$ -minor, that is, its Alexander polynomial is a **polynomial**, not a Laurent polynomial.

The set of linear representations, or conjugacy classes of representations are important subject to study in the low dimensional topology.

Here we consider them over a **finite prime field** \mathbb{Z}/p .

- The set of all $SL(2, \mathbb{Z}/p)$ -representations is an algebraic set over a finite field \mathbb{Z}/p .
- It is not easy to check whether the set of representations is **empty** or not, because to solve a polynomial equation over a finite field is very difficult.

Suzuki-Kitano (to appear in JKTR) computed the followings for the [Reidemeister-Rolfsen's list](#);

The number of

- the number of the conjugacy classes of $SL(2, \mathbb{Z}/p)$ -representations,
- the number of the conjugacy classes of non abelian $SL(2, \mathbb{Z}/p)$ -representations,
- the number of the conjugacy classes of surjective $SL(2, \mathbb{Z}/p)$ -representations,

where p is a prime number with $p \leq 23$.

表 1: Number of non abelian representations

K	2	3	5	7	11	13	17	19	23
3_1	1	4	10	14	18	30	44	38	42
4_1	0	4	8	20	16	28	28	32	36
6_2	0	0	0	4	4	26	36	36	34
6_3	0	0	4	8	32	12	24	40	40
7_1	0	0	0	12	0	78	0	0	0
7_5	0	0	0	8	8	8	28	28	40
8_{12}	0	0	0	0	12	4	12	24	28
8_{18}	4	20	48	84	112	308	300	248	340
9_9	0	0	0	12	6	32	32	32	32
9_{48}	4	0	20	64	60	132	194	138	200
10_{98}	4	20	84	200	340	692	870	870	1352
10_{99}	4	20	128	320	736	1368	1832	2176	2984
10_{124}	0	0	16	0	88	0	0	152	0

There are lots of zeros. It is hard to see the law on the numbers at first glance.

Then we consider

Problem 1.1. *Does there exist a non abelian representation*

$$G(K) \rightarrow SL(2, \mathbb{Z}/p)$$

for infinitely many prime numbers p ?

By using the classical theory by de Rham:

G. De Rham, Introduction aux polynomes d'un nœud,
L'Enseignement Mathématique, Vol.13 (1967),
we can prove the following.

Theorem 1.2. *If $\Delta_K(t) \neq 1$, then there exists a non abelian representation $G(K) \rightarrow SL(2, \mathbb{Z}/d)$ for infinitely many $d \in \mathbb{Z}_+$.*

Remark 1.3. *Here we do not know whether we can choose infinitely many prime numbers in the set of d 's.*

If $\Delta_K(t)$ has a special form, we can prove the following.

Theorem 1.4. *If $\Delta_K(t)$ is a degree 2 polynomial, then there exist a non abelian representation $G(K) \rightarrow GL(2, \mathbb{Z}/p)$ for infinitely many prime numbers $p \in \mathbb{Z}_+$.*

Corollary 1.5. *If $\Delta_K(t) = f(t)g(t)$ with the degree of $f(t)$ is two and $f(1) = 1$, then there exists a non abelian representation $G(K) \rightarrow GL(2, \mathbb{Z}/p)$ for infinitely many prime numbers $p \in \mathbb{Z}_+$.*

2 Theorem of de Rham

Recall the theorem by de Rham.

We fix a Wirtinger presentation of K as

$$G(K) = \langle x_1, \dots, x_n \mid r_1, \dots, r_{n-1} \rangle.$$

Now we take a map

$$\varphi : \{x_1, \dots, x_n\} \ni x_i \mapsto \begin{pmatrix} a & b_i \\ 0 & 1 \end{pmatrix} \in GL(2; \mathbb{C})$$

where $a \neq 0 \in \mathbb{C}$ and $b_1, \dots, b_n \in \mathbb{C}$.

When φ can be extended to $G(K)$ as a homomorphism?

Remark 2.1. *If $b_1 = \cdots = b_n = b \in \mathbb{C}$, then it can be done as an abelian representation:*

$$\varphi : G(K) \ni x_i \mapsto \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in GL(2; \mathbb{C}).$$

Hence we assume that

$$\mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \neq c \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}.$$

Under the fixing presentation, we have the Alexander matrix

$$A \in M((n - 1) \times n; \mathbb{Z}[t, t^{-1}]),$$

and by putting $t = a$,

$$A(a) \in M((n - 1) \times n; \mathbb{C}).$$

Theorem 2.2 (de Rham). *The map*

$$\varphi : \{x_1, \dots, x_n\} \ni x_i \mapsto \begin{pmatrix} a & b_i \\ 0 & 1 \end{pmatrix} \in GL(2; \mathbb{C})$$

can be extended to $G(K)$ as a homomorphism if and only if $A(a)\mathbf{b} = \mathbf{0}$. In particular then it holds $t = a$ is a zero of $\Delta_K(t) = 0$.

Outline of Proof:

A map φ can be extended to the $G(K)$ as a homomorphism if and only if any relator maps to the identity matrix E .

For example, we take one relator

$$r_i = x_i x_j x_i^{-1} x_k^{-1}.$$

Then the condition;

$$\begin{aligned}\varphi(r_i) &= \varphi(x_i)\varphi(x_j)\varphi(x_i)^{-1}\varphi(x_k)^{-1} \\ &= E\end{aligned}$$

is equivalent to

$$\varphi(x_i)\varphi(x_j) = \varphi(x_k)\varphi(x_i).$$

Then we compute the both sides:

$$\varphi(x_i)\varphi(x_j) = \begin{pmatrix} a & b_i \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b_j \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a^2 & ab_j + b_i \\ 0 & 1 \end{pmatrix}$$

$$\varphi(x_k)\varphi(x_i) = \begin{pmatrix} a & b_k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b_i \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a^2 & ab_i + b_k \\ 0 & 1 \end{pmatrix}.$$

By comparing entries of the both, we have

$$ab_j + b_i = ab_i + b_k,$$

and then

$$ab_j + (1 - a)b_i - b_k = 0.$$

Here we consider b_1, b_2, \dots, b_n are the variables.

This condition can be also given by Fox's free differential calculus as follows.

$$\alpha_* \left(\frac{\partial}{\partial x_i} (x_i x_j - x_k x_i) \right) = 1 - t$$

$$\alpha_* \left(\frac{\partial}{\partial x_j} (x_i x_j - x_k x_i) \right) = t$$

$$\alpha_* \left(\frac{\partial}{\partial x_k} (x_i x_j - x_k x_i) \right) = -1.$$

Then the above condition is the same with the i -th entry of the vectort $A(a)\mathbf{b}$ equals zero.

Therefore the condition for φ to be extended is given by the linear system

$$A(a)\mathbf{b} = \mathbf{0}.$$

By the linear algebra, there exists $\mathbf{b} \neq \mathbf{0}$ if and only if any $(n - 1) \times (n - 1)$ -minors of $A(a)$ is zero.

Hence, when \mathbf{b} exists, $t = a$ is a zero of $\Delta_K(t) = 0$. Then

$$\varphi : \{x_1, \dots, x_n\} \ni \mapsto \begin{pmatrix} a & b_i \\ 0 & 1 \end{pmatrix} \in GL(2, \mathbb{C})$$

can be extended to $G(K)$ as a homomorphism.

Remark 2.3. Because the condition $A(a)\mathbf{b} = \mathbf{0}$ is a *linear condition*, if we find some a and \mathbf{b} , then for any $s \in \mathbb{C} - \{0\}$,

$$\varphi_s : \{x_1, \dots, x_n\} \ni \begin{pmatrix} a & sb_i \\ 0 & 1 \end{pmatrix} \mapsto \in GL(2, \mathbb{C})$$

gives a representation.

Then φ_s is a deformation of the direct sum of an abelian representation

$$G(K) \ni x_i \mapsto a \in \mathbb{C}$$

and the 1-dimensional trivial representation

$$G(K) \ni x_i \mapsto 1 \in \mathbb{C}$$

into an affine representation in $GL(2; \mathbb{C})$.

Here we consider a map into $SL(2; \mathbb{C})$.

Take a map

$$\hat{\varphi} : \{x_1, \dots, x_n\} \rightarrow SL(2; \mathbb{C})$$

is given by $\hat{\varphi}(x_i) = \begin{pmatrix} a & b_i \\ 0 & a^{-1} \end{pmatrix}$.

Starting from $\hat{\varphi}$, by the similar computation, the condition to be extended for $\hat{\varphi}$ is given by

$$A(a^2)\mathbf{b} = 0.$$

In particular at that time,

$$\Delta_K(a^2) = 0,$$

that is, $t = a^2$ is a zero of $\Delta_K(t) = 0$.

3 Construction of a homomorphism of $G(K)$ into symmetric groups

From the above observation, we can get also a homomorphism of $G(K)$ into symmetric groups.

Originally this argument was given in the famous paper by

- R. H. Fox, A quick trip through knot theory, Topology of 3-Manifolds edited by Fort.

We recall

- $\Delta_K(t)$ is well defined up to $\pm t^k$.
- It means a special value of $\Delta_K(t)$ is not well-defined as a knot invariant.

However we consider $|\Delta_K(m)|$ as a number, not invariant, under fixing Wirtinger presentation for any integer $m \in \mathbb{Z}$.

Remark 3.1. *We choice $\Delta_K(t)$ to be a polynomial as a minor of A by changing a presentation of $G(K)$.*

First example is the knot determinant $d_K = |\Delta_K(-1)| \in \mathbb{Z}$.

Remark 3.2. *It is known that $|\Delta_K(-1)| \neq 0$ and it is a knot invariant.*

By substituting $t = -1$, we get

$$A(-1) \in M((n-1) \times n; \mathbb{Z}).$$

Then the linear equation system for the extension is defined over \mathbb{Z} and clearly it has **no nontrivial solution**, because

$$|\Delta_K(-1)| = d_K \neq 0.$$

However if we consider and treat

$$A(-1)\mathbf{b} \equiv \mathbf{0}$$

over \mathbb{Z}/d_K , clearly any $(n-1) \times (n-1)$ -minor of $A(-1)$ is zero mod d_K . Hence there exists the solution

$$\mathbf{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in (\mathbb{Z}/d_K)^n.$$

Then we can get a representation

$$\bar{\varphi} : G(K) \ni x_i \mapsto \begin{pmatrix} -1 & b_i \\ 0 & 1 \end{pmatrix} \in GL(2; \mathbb{Z}/d_K).$$

Here an affine transformation

$$\bar{\varphi}(x_i) = \begin{pmatrix} -1 & b_i \\ 0 & 1 \end{pmatrix}$$

can be consider a permutation on \mathbb{Z}/d_K :

$$\mathbb{Z}/d_K \ni m \mapsto -m + b_i \in \mathbb{Z}/d_K.$$

Therefore we obtain a homomorphism;

$$G(K) \rightarrow \mathfrak{S}_{d_K}.$$

From here we consider $t = m \in \mathbb{Z}$ and $d_{K,m} = |\Delta_K(m)|$.
Here if $d_{K,m}$ is not prime. we put some assumption:

$$(m, d_{K,m}) = 1.$$

In this case,

- m is a unit in $\mathbb{Z}/d_{K,m}$.
- the linear sytem:

$$A(m)\mathbf{b} \equiv \mathbf{0} \pmod{d_{K,m}}$$

has a solution over $\mathbb{Z}/d_{K,m}$.

By finding a solution a and \mathbf{b} , we obtain a representation

$$\bar{\varphi} : G(K) \rightarrow GL(2; \mathbb{Z}/d_{K,m}).$$

For any generator x_i , its image

$$\bar{\varphi}(x_i) = \begin{pmatrix} m & b_i \\ 0 & 1 \end{pmatrix}$$

gives a permutation:

$$\mathbb{Z}/d_{K,m} \ni k \mapsto mk + b_i \in \mathbb{Z}/d_{K,m}.$$

Therefore we obtain a homomorphism of $G(K)$;

$$G(K) \rightarrow \mathfrak{S}_{d_{K,m}}.$$

4 Example: Trefoil knot

Here we consider $K = 3_1$, the trefoil knot. We take and fix the following presentation:

$$G(K) = \langle x, y \mid xyx = yxy \rangle$$

By applying the Fox's free derivatives $\frac{\partial}{\partial x}$, $\frac{\partial}{\partial y}$, we get

- $A = \begin{pmatrix} t^2 - t + 1 & -t^2 + t - 1 \end{pmatrix}$,
- $\Delta_{3_1}(t) = t^2 - t + 1$.

Example 4.1. *First we consider the case of $t = -1$.*

$$d_{3_1} = |\Delta_K(-1)| = 3.$$

Then we find a solution

$$A(3) \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \equiv \mathbf{0} \pmod{3}.$$

In this case, the Alexander matrix mod 3 :

$$A(3) \equiv \begin{pmatrix} 0 & 0 \end{pmatrix} \pmod{3}.$$

Then

- *any $n \in \mathbb{Z}/3$ is zero of $\Delta_{3_1}(t) \equiv 0 \pmod{3}$,*
- *any $\mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \in (\mathbb{Z}/3)^2$ is a solution.*

For examples, taking $n = 2$ and $b_1 = 1, b_2 = 0$, we can define a representation

$$\varphi : G(3_1) \rightarrow GL(2, \mathbb{Z}/3)$$

by

$$\varphi(x) = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \varphi(y) = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}.$$

Furthermore, if we define a map

$$\hat{\varphi} : \{x, y\} \rightarrow SL(2, \mathbb{Z}/3)$$

by

$$\hat{\varphi}(x) = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}, \hat{\varphi}(y) = \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix},$$

it gives a representation

$$\hat{\varphi} : G(3_1) \rightarrow SL(2, \mathbb{Z}/3).$$

We put $m = 2$ and then obtain $d_2 = |\Delta(2)| = 3$. Then we have the same as above.

Example 4.2. *If we put $m = 3$, then $d_3 = |\Delta_{3_1}(3)| = 7$. In this case any n and any \mathbf{b} satisfies also the linear equation, because*

$$A(3) = \begin{pmatrix} 0 & 0 \end{pmatrix} \text{ mod } 7.$$

Hence we obtain a representation

$$\varphi : G(3_1) \rightarrow GL(2, \mathbb{Z}/7)$$

and

$$\hat{\varphi} : G(3_1) \rightarrow SL(2, \mathbb{Z}/7).$$

For examples,

$$\hat{\varphi}(x) = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}, \hat{\varphi}(y) = \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix}$$

gives a representation

$$\hat{\varphi} : G(K) \rightarrow SL(2, \mathbb{Z}/7).$$

Finally we can see

Proposition 4.3. *There exist a **non abelian** representation of $G(3_1)$ in $SL(2, \mathbb{Z}/d)$ for **infinitely many integers** d .*

5 $SL(2, \mathbb{Z}/d)$ -representation of $G(K)$

In this section, we consider the following problem.

Problem 5.1. Does there exist a *non abelian* representation $G(K) \rightarrow SL(2, \mathbb{Z}/d)$ for *infinitely many integer* d ?

For simplicity we suppose

- The Alexander polynomial is given to be

$$\Delta_K(t) = a_{2k}t^{2k} + a_{2k-1}t^{2k-1} + \cdots + a_1t + a_0,$$

where $a_{2k} = a_0 > 0$, $\sum_{i=0}^{2k} a_i = \pm 1$.

If we substitute $t = p^2$ for $\Delta_K(t)$, then

$$d_p = \Delta_K(p^2) = a_{2k}p^{4k} + a_{2k-1}p^{4k-2} + \cdots + a_1p^2 + a_0.$$

If p is a **sufficient large prime number**,

$$d_{p^2} = \Delta_K(p^2) > p^2 > p.$$

Further we put the condition $(a_0, p) = 1$, then

$$\Delta_K(p^2) \equiv a_0 \pmod{p}.$$

Hence

$$(\Delta_K(p^2), p) = 1.$$

Then for any prime number p as above, p and p^2 are **units** in \mathbb{Z}/d_p .

Because there exists a solution

$$A(p^2)\mathbf{b} \equiv \mathbf{0} \pmod{d_{p^2}},$$

then a non abelian representation

$$\tilde{\rho} : G(K) \ni x_i \mapsto \begin{pmatrix} p & b_i \\ 0 & p^{-1} \end{pmatrix} \in SL(2, \mathbb{Z}/d_{p^2})$$

is obtained.

Therefore we obtain the following.

Theorem 5.2. *There exists a non abelian representation $G(K) \rightarrow SL(2, \mathbb{Z}/d_{p^2})$ for infinitely many $d_{p^2} = |\Delta_K(p^2)|$.*

Remark 5.3. *We do not know whether d_{p^2} is a prime number or not.*

6 $GL(2, \mathbb{Z}/p)$ -representation of $G(K)$

We want to discuss representation in $SL(2, \mathbb{Z}/p)$ where p is a prime number. Namely the following is the original problem:

Problem 6.1. *Does there exist a non commutative representation $G(K) \rightarrow SL(2, \mathbb{Z}/p)$ for infinitely many prime number p ?*

Here we put some restriction on $\Delta_K(t)$ and further consider $GL(2, \mathbb{Z}/p)$ -representations.

That is, the problem is as follows:

Problem 6.2. *Does there exist a non abelian representation $G(K) \rightarrow GL(2, \mathbb{Z}/p)$ for infinitely many prime number p ?*

For any knot K with the Alexander polynomial of degree 2, we can give the answer as follows.

Now we assume that the Alexander polynomial of K is given by

$$\Delta_K(t) = at^2 - bt + a,$$

where $b \geq a > 0$, $\Delta_K(1) = 2a - b = \pm 1$. Then by the condition $2a - b = \pm 1$,

$$a = \frac{b \pm 1}{2}.$$

Now we can prove the following.

Proposition 6.3. *There exists a solution of the congruence $\Delta_K(t) \equiv 0 \pmod{p}$ for infinitely many prime number p .*

If $\Delta_K(n) \equiv 0 \pmod{p}$, then we can find a non trivial solution \mathbf{b} of $A(n)\mathbf{b} \equiv \mathbf{0} \pmod{p}$. Then

$$\rho : G(K) \ni x_i \mapsto \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \in GL(2, \mathbb{Z}/p)$$

gives a non abelian representation.

Theorem 6.4. *There exist a non abelian representation $G(K) \rightarrow GL(2, \mathbb{Z}/p)$ for infinitely many prime number p .*

Let us consider the congruence

$$at^2 - bt + a \equiv 0 \pmod{p}.$$

When we consider the equation

$$at^2 - bt + a = 0$$

over \mathbb{C} , then

$$t = \frac{b \pm \sqrt{b^2 - 4a^2}}{2a}$$

is the solutions. Here if $D = b^2 - 4a$ is a square number mod p , that is, a quadratic residue mod p , then there exists a solution of the above congruence.

Definition 6.5. For k and a prime number p , the Legendre symbol $\left(\frac{k}{p}\right)$ is defined as follows.

$$\left(\frac{k}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv k \pmod{p} \text{ has a solution} \\ -1 & \text{if } x^2 \equiv k \pmod{p} \text{ has no solution} \end{cases}$$

By using $2a - b = \pm 1$, we can eliminate a in $D = b^2 - 4a^2$ and obtain $D = \pm 2b - 1$. Then we put $D_+ = 2b - 1$ and $D_- = -2b - 1$ for the both.

By using Legendre symbol, we can state the following.

Proposition 6.6. *For infinitely many prime numbers p , Legendre symbols of $D = D_+, D_+ \pmod p$ is*

$$\left(\frac{D}{p}\right) = 1.$$

1. The case of $D_+ = 2b - 1$.

Here we assume that

$$p = 4(2b - 1)n + 1$$

is a prime number and p is not a divisor of a .

Remark 6.7. *By the theorem of Dirichlet, there exist infinitely many prime number as above.*

If p is a divisor of $2b - 1$, then $D_+ \equiv 0 \pmod{p}$. Hence there exists a solution of $\Delta_K(t) \equiv 0 \pmod{p}$.

Assume that p is not a divisor of $2b - 1$.

By the reciprocity law of the Jacobi symbol,

$$\begin{aligned}\left(\frac{2b-1}{p}\right)\left(\frac{p}{2b-1}\right) &= (-1)^{\frac{p-1}{2} \frac{2b-1-1}{2}} \\ &= (-1)^{2(2b-1)n(b-1)} \\ &= 1.\end{aligned}$$

Therefore

$$\begin{aligned}\left(\frac{2b-1}{p}\right) &= \left(\frac{p}{2b-1}\right) \\ &= \left(\frac{4(2b-1)n+1}{2b-1}\right) \\ &= \left(\frac{1}{2b-1}\right) \\ &= 1\end{aligned}$$

2. The case of $D_- = -2b - 1$

Now assume that

$$p = 4(2b + 1)n + 1$$

is a prime number and is not a divisor of a .

Now

$$\left(\frac{-2b - 1}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{2b + 1}{p}\right).$$

By the quadratic reciprocity law,

$$\begin{aligned} \left(\frac{-1}{p}\right) &= (-1)^{\frac{p-1}{2}} \\ &= (-1)^{2(2b+1)n} \\ &= 1. \end{aligned}$$

Hence

$$\left(\frac{-2b-1}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{2b+1}{p}\right) = \left(\frac{2b+1}{p}\right).$$

By using the reciprocity law of the Jacobi symbol,

$$\begin{aligned} \left(\frac{2b+1}{p}\right) \left(\frac{p}{2b+1}\right) &= (-1)^{\frac{p-1}{2} \frac{2b+1-1}{2}} \\ &= (-1)^{2(2b+1)nb} \\ &= 1. \end{aligned}$$

Therefore we have

$$\begin{aligned}\left(\frac{2b+1}{p}\right) &= \left(\frac{p}{2b+1}\right) \\ &= \left(\frac{4(2b+1)n+1}{2b+1}\right) \\ &= \left(\frac{1}{2b+1}\right) \\ &= 1.\end{aligned}$$