ORBIT OF QUADRATIC IRRATIONALS MODULO P BY THE MODULAR GROUP

Shin-Ichi Katayama[1], Toru Nakahara[2], Syed Inayat Ali Shah[3], Mohammad Naeem Khalid[3] and Sareer Badshah[3]
[1]*1Tokushima University, Japan.*
[2]*Saga University, Japan.*
[3]*Islamia College University, Peshawar (N.W.F.P) Pakistan.*

ABSTRACT

Let p be an odd prime number, and α be a solution of an irreducible quadratic equation $x^2+ax+b=0$ over the rationals Q**.** In Mushtaq study, the behavior of orbits of a quadratic irrational in a quadratic field $Q(\alpha)$ by the special linear transformation group $SL(2,Z)$ modulo $\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\right\}$ is investigated, where; Z denotes the ring of rational integers (Mushtaq, 1988). In this study, the above group is denoted by $PSL(2,Z)$, presented as the projective special linear transformation group. Let α be a root of quadratic equation $x^2-x-1\equiv 0$ (mod p), then we shall introduce the orbit of the (irrational) element α in a finite field $F_p[\alpha]$ by $PSL(2,F_p)$, where F_p equal to Z/pZ.

INTRODUCTION

Let p be an odd prime number and F_p be the finite field of p elements $\{0,1,\cdots\cdots p-1\}$. In this case, an element j in the field F_p and the representative number $j(0\leqq j\leqq p-1)$ in a class $\{a\in Z; a\equiv j(\text{mod } p)\}$ in the residue class field Z/pZ modulo p, where Z denotes the ring of rational integers. $Q(\sqrt{d})$ be a real quadratic number field over the rationals Q with non-square integer $d\geqq 2$.

In this article, we investigate an analogue in the quadratic extension of the finite field F_p to a result on the orbits of quadratic irrationals in a global field $Q(\sqrt{d})$ (Mushtaq, 1988).

Mushtaq (1988) showed Fig. modulo 13, where the diagram is one orbit of length 13 in the disjoint orbit decomposition for the quadratic extension $F_{13}(\alpha)$ over the prime field F_{13} acting on the modular group $SL(2,F_{13})$. The present study presents another orbit of length 156 given in theorem 2.

In the figure below, two points 5, 8 are fixed by X, and two points 4,10 by Y in $SL(2,F_{13})$, where $X=\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ and $Y=\begin{pmatrix}1&-1\\1&0\end{pmatrix}$.

To classify the finite field $F_p(\alpha)$ according to the number of orbits in the field, where α is a root of a quadratic equation $x^2+ax+b=0$; this study uses Quadratic Reciprocity Law to deal with the above mentioned problem.

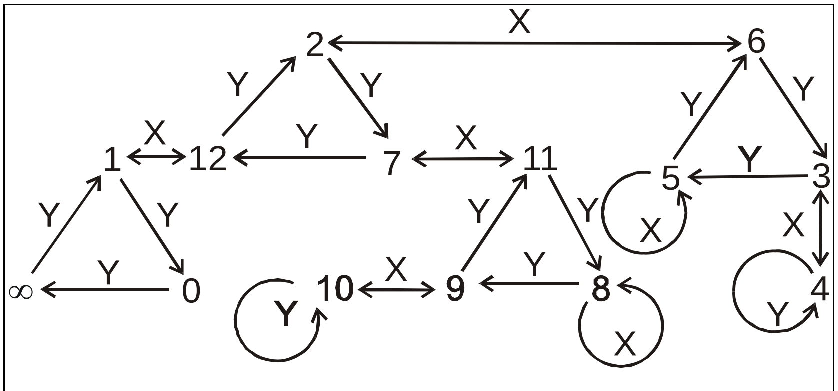

Fig. Modulo 13

RESULTS AND DISCUSSION

Two cases of odd prime numbers were considered, the details of as follows:

Case No. 1: $p \equiv 1, 4 (\mathrm{mod}\ 5)$.

Let D be the discriminant of the quadratic equation $f(x) = x^2 - x - 1 = 0$. Using the first supplementary and quadratic reciprocity law, we have

$$\left(\frac{D}{p}\right) = \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{\pm 1}{5}\right) = 1.$$

The equation $f(x) = 0$ is decomposed in the linear factors in F_p

$$f(x) = (x - a)(x - \bar{a}),$$

where $a = \dfrac{1+\sqrt{D}}{2} = \dfrac{1+c}{2}$, $\bar{a} = \dfrac{1-c}{2}$.

The field $F_p(\alpha) = s\alpha + t;\ s, t \in F_p$ coincides with F_p, namely in the case of $p \equiv 1, 4 (\mathrm{mod}\ 5)$, and the field extension $F_p(\alpha)$ over F_p does not occur.

Let F_p^x be the multiplicative group in F_p, the special linear transformation group $SL(2, F_p)$, is generated by

$$X = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } Y = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$$

modulo $\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right\}$ in Mushtaq (1988).

Using the two equations $X\begin{pmatrix} \omega \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ \omega \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \omega \\ 1 \end{pmatrix}$ and $Y\begin{pmatrix} \omega \\ 1 \end{pmatrix} = \begin{pmatrix} \omega - 1 \\ \omega \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \omega \\ 1 \end{pmatrix}$ for $\omega \in Q(\alpha)$, we identify a vector $\begin{pmatrix} \beta \\ \gamma \end{pmatrix}$ and the ratio $\dfrac{\beta}{\gamma}$ for elements $\beta, \gamma \in F_p(\alpha)$.

Hence $S(\beta)$ means $S\begin{pmatrix} \beta \\ 1 \end{pmatrix}$ for any transformation $S \in SL(2, F_p)$. Then

By $X^2(\omega) = X\left(\dfrac{-1}{\omega}\right) = \omega,$ and $Y^2(\omega) = Y\left(\dfrac{\omega - 1}{\omega}\right) = \dfrac{-1}{\omega - 1}$

$Y^3(\omega) = Y\left(\dfrac{-1}{\omega - 1}\right) = \omega$. Hence the order of X and Y is 2 and 3 respectively.

As

$$XY^2(\omega) = XY\left(\frac{\omega-1}{\omega}\right) = X\left(\frac{-1}{\omega-1}\right) = \omega - 1$$

Hence,

$$\left(XY^2\right)^{-1}(\omega) = Y^{-2}X^{-1}(\omega) = YX(\omega) = \omega + 1$$

Then it follows that

$$1 \xrightarrow{YX} 2 \xrightarrow{YX} 3 \cdots$$
$$\cdots \xrightarrow{YX} p-1 \xrightarrow{YX} 0 \xrightarrow{YX} 1.$$

Therefore, in the case of $p \equiv 1, 4 \pmod 5$, we get a single orbit by the action of $PSL(2, F_p)$.

Case No. 2: $p \equiv 2, 3 \pmod 5$.

For any prime $p \equiv 2, 3 \pmod 5$, the discriminant $D = 5$ is not square in F_p.

Thus the field

$$F_p(\alpha) = \{s\alpha + t;\ s, t \in F_p(\alpha)\}$$

is the quadratic extension over F_p. To determine the orbits by the action of $PSL(2, F_{p.})$, we proceed as follows:

i). For any element a of F_p, and taking the parallel transformation YX, the closed circuit

$$a \xrightarrow{YX} a+1 \xrightarrow{YX} \cdots$$
$$\cdots \xrightarrow{YX} a-1 \xrightarrow{YX} a$$

makes an orbit.

ii). Next, assume that a rational element $a \in F_p$ and an irrational $\beta \in F_p(\alpha) \setminus F_p$ belong to the same orbit. Then there exists a transformation $S = \begin{pmatrix} s & t \\ u & v \end{pmatrix} \in SL(2, F_p)$ such that $S(a) = \beta$ for $\beta = b\alpha + c,\ b \neq 0, c \in F_p$, we have $\beta = b\alpha + c$ for $\beta = \dfrac{sa+t}{ua+v} \in F_p$, however $b\alpha + c \notin F_p$, which is a contradiction.

iii). Finally, we show that any two irrationals β and γ belong to the same orbit. For two irrationals $\beta = b\alpha + c$ and $\gamma = d\alpha + f \in F_p(\alpha)$;

$b \neq 0,\ c,\ d \neq 0, f \in F_p$, it shows that there exists $S \in SL(2, F_p)$ such that $S(\beta) = \gamma$.

Taking the parallel transformation $\left(XY^2\right)^{-1} = YX : \beta \mapsto \beta + 1$ denoted by Z. Since $Z^{-h}(\delta) = g\alpha$ for $\delta = g\alpha + h$, put $S(b\alpha) = d\alpha$. We obtain $S(b\alpha) = d\alpha$ iff $S'(\alpha) = b^{-1}d\alpha$ for $S = \begin{pmatrix} s & t \\ u & v \end{pmatrix}$ and

$$S' = \begin{pmatrix} b^{-1}sb & b^{-1}t \\ ub & v \end{pmatrix} \in SL(2, F_p).$$

Now it is enough to show that $S(\alpha) = \dfrac{s\alpha + t}{u\alpha + v} = d\alpha$ with $sv - tu = 1$ for a suitable transformation S, namely

$$\frac{(s\alpha + t)(u\bar{\alpha} + v)}{(u\alpha + v)(u\bar{\alpha} + v)}$$

$$= \frac{su(-1) + su\alpha + tu(1-\alpha) + tv}{u^2(-1) + uv + v^2}$$

$$= \frac{\alpha - su + tu + tv}{g(u, v)} = d\alpha$$

with $g(u, v) = -u^2 + uv + v^2$.

For $d_0 = d^{-1}$ we seek for a rational solution $\{u, v\}$ in F_p such that $g(u, v) = d_0$, which implies that $v^2 + uv - (u^2 + d_0) = 0$.

Let $D_v = u^2 + 4(u^2 + d_0) = 5u^2 + 4d_0$ be the discriminant of the above quadratic equation on v, then iii)$_0$. If d_0 is a square e_0^2 in F_p, then we find a solution $\{s,t,u,v\} = \{e_0^{-1}, 0, 0, e_0\}$.

iii)$_1$. We assume that d_0 is not square free in F_p for $p \equiv 2, 3 \pmod 5$, 5 is not square free. Denoting a generator of the multiplicative group F_p^x, namely a primitive root modulo p by r.

By our assumption, d_0 is not a square in F_p^x, assuming the discriminant $D_v = 5u^2 + 4d_0$ is not a square for any $u = r^j \in F_p^x$, we obtained $r^{2a+1}r^{2j} + r^{2d+1} = r^{2kj+1}$.

If $r^{2kj+1} = r^{2k\ell+1}$, namely $2k_j + 1 \equiv 2k_\ell + 1 \pmod{p-1}$, then $r\ 2j \equiv r^{2\ell} \pmod p$, hence $2j \equiv 2\ell \pmod{p-1}$, $j = \ell$ holds for $0 \leqq j - \ell \leqq \dfrac{p-3}{2}$.

For $m\left(0 \leqq m \leqq \dfrac{p-3}{2}\right)$, we have $r^{2k_m+1} = r^{2d+1}$, namely $r^{2a+1}r^{2m} + r^{2d+1} = r^{2d+1}$, hence $r^{2a+1}r^{2m} = 0$, which is a contradiction.

There exists $j\left(0 \leqq j \leqq \dfrac{p-3}{2}\right)$ such that $u = r^i$ and $5u^2 + 4d_0 = r^{2kj}$, we obtain $\sqrt{D_v} = r^{kj}$.

Finally, we determine the transformation $S = \begin{pmatrix} s & t \\ u & v \end{pmatrix}$, with

$v = \dfrac{-u_0 + \sqrt{D_v}}{2}, \sqrt{D_v} = e_0$, where

$v = \dfrac{-u_0 + e_0}{2}$, $e_0 = \sqrt{D_v}$, and

$D_v = 5u_0^2 + 4d^{-1} = e_0^2, e_0 \in F_p$

$sv - tu_0 = 1$.

If u_0 or $v_0 \in F_p^x$, there exists a solution $\{s, t, u, v\} = \{0, -u_0^{-1}, u_0, v_0\}$ or $\{v_0^{-1}, 0, u_0, v_0\}$ with $sv - tu = 1$. In the case, if $u_0 = v_0 = 0$, then $0 = \dfrac{0 + e_0}{2}$, hence by $e_0 = 0$, and by $5.0 + 4 \cdot d_0 = 0$, we get $d_0 = d^{-1} = 0$, which is a contradiction.

Then by the transformation $Z^{-d_0^{-1}(-su+tu+tv)}$ to $S(\alpha)$, it was obtained $ZS(\alpha) = d\alpha$, namely α and $d\alpha$ belongs to the same orbit. Therefore the following theorem was obtained.

Theorem. Let p be an odd prime and α be a solution of a quadratic equation $x^2 - x - 1 = 0$. Let $F_p(\alpha)$ be the field $\{s\alpha + t;\ s, t \in F_p\}$ over the finite prime field $F_p = \{0, 1, \cdots p-1\}$, then:

(1) For $p \equiv 1, 4 \pmod 5$ we have $F_p(\alpha) = F_p$ and F_p is occupied by the single orbit of the length p by the action of $PSL(2, Z)$;
$0 \to 1 \to \cdots \to p-1 \to 0$.

(2) For $p \equiv 2, 3 \pmod 5$ we have the quadratic extension $F_p(\alpha)$ over F_p and $F_p(\alpha)$ is separated into two disjoint orbits, namely one is F_p of the length p;
$0 \to 1 \to \cdots \to p-1 \to 0$

and the other $F_p(\alpha)\backslash F_p$ of the length p^2-p by the action of $PSL(2,F_p)$; the details of these are presented in the diagram below:

$$
\begin{array}{ccccccc}
\alpha & \to & \alpha+1 & \to & \cdots & \to & \alpha+p-1 \\
 & & & & & & \downarrow \\
2\alpha & \leftarrow & 2\alpha+1 & \leftarrow & \cdots & \leftarrow & 2\alpha+p-1 \\
\downarrow & & & & & & \\
3\alpha & \to & 3\alpha+1 & \to & \cdots & \to & 3\alpha+p-1 \\
 & & & & & & \downarrow \\
\cdot & \leftarrow & \cdots & \leftarrow & \cdots & \leftarrow & \cdot \\
\downarrow & & & & & & \\
\cdot & \to & \cdots & \to & \cdots & \to & \cdot \\
(p-1)\alpha & \leftarrow & (p-1)\alpha+1 & \leftarrow & \cdots & \leftarrow & (p-1)\alpha+p-1 \\
\downarrow & & & & & & \\
\alpha. & & & & & &
\end{array}
$$

REFERENCES

Kuroki A (2007). On quadratic reciprocity law. (Bachelor Thesis), Tokushima University, Japan.

Mushtaq Q (1988). Modular group acting on real quadratic fields. Bulletin Australian Mathematical Society. (37):303-309.

Takagi T (1903). A simple proof of the quadratic reciprocity law for quadratic residues. Proc. Phys. –Math. Soc. Japan. Ser II, (2):74-78.

Tomonou D (2006). Modulser group which acts on real quadratic fields (Master Thesis). Saga University, Japan.