ORBIT OF QUADRATIC IRRATIONALS MODULO P BY THE MODULAR GROUP

Shin-Ichi Katayama¹, Toru Nakahara², Syed Inayat Ali Shah³, Mohammad Naeem Khalid³ and Sareer Badshah³
¹Tokushima University, Japan.
²Saga University, Japan.
³Islamia College University, Peshawar (N.W.F.P) Pakistan.

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

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

In this article, we investigate an analogue in the quadratic extension of the finite field \( \mathbb{F}_p \) to a result on the orbits of quadratic irrationals in a global field \( \mathbb{Q}(\sqrt{\mathbb{d}}) \) (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 \( \mathbb{F}_{13}(\alpha) \) over the prime field \( \mathbb{F}_{13} \) acting on the modular field \( \text{SL}(2, \mathbb{F}_{13}) \). 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 \( \text{SL}(2, \mathbb{F}_{13}) \), 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 \( \mathbb{F}_p(\alpha) \) according to the number of orbits in the field, where \( \alpha \) 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.
RESULTS AND DISCUSSION

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

Case No. 1: \( p \equiv 1, 4 \pmod{5} \).

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

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

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

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

where

\[
a = \frac{1 + \sqrt{D}}{2} = \frac{1 + c}{2},
\]

\[
\bar{a} = \frac{1 - c}{2}.
\]

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

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

\[
X = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad Y = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}
\]

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

Using the two equations

\[
X \begin{pmatrix} \omega \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \omega \\ 1 \end{pmatrix} \quad \text{and} \quad Y \begin{pmatrix} \omega \\ 1 \end{pmatrix} = \begin{pmatrix} \omega - 1 \\ \omega \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \omega \\ 1 \end{pmatrix}
\]

for \( \omega \in \mathbb{Q}(\alpha) \), we identify a vector \( \begin{pmatrix} \beta \\ \gamma \end{pmatrix} \) and the ratio \( \frac{\beta}{\gamma} \) 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

\[
X^2(\omega) = X \begin{pmatrix} -1 \\ \omega \end{pmatrix} = \omega,
\]

By

\[
Y^2(\omega) = Y \begin{pmatrix} \omega - 1 \\ \omega \end{pmatrix} = \begin{pmatrix} -1 \\ \omega - 1 \end{pmatrix}
\]

and

\[
Y^3(\omega) = Y \begin{pmatrix} -1 \\ \omega - 1 \end{pmatrix} = \omega.
\]

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,
\[\left(\frac{XY^2}{\omega}\right)^{-1}(\omega) = Y^{-2}X^{-1}(\omega) = YX(\omega) = \omega + 1\]
Then it follows that
\[\begin{array}{cccccc}
1 & \xrightarrow{YX} & 2 & \xrightarrow{YX} & 3 & \ldots \\
\ldots & \xrightarrow{YX} & p-1 & \xrightarrow{YX} & 0 & \xrightarrow{YX} 1
\end{array}\]
Therefore, in the case of \(p \equiv 1, 4 \text{ (mod 5)}\), we get a single orbit by the action of \(\text{PSL}(2, F_p)\).

**Case No. 2: \(p \equiv 2, 3 \text{ (mod 5)}\).**
For any prime \(p \equiv 2, 3 \text{ (mod 5)}\), 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 \(\text{PSL}(2, F_p)\), we proceed as follows:

i). For any element \(a \in F_p\), and taking the parallel transformation \(YX\), the closed circuit
\[\begin{array}{c}
a \xrightarrow{YX} a + 1 \xrightarrow{YX} \ldots \\
\ldots \xrightarrow{YX} a - 1 \xrightarrow{YX} a
\end{array}\]
makes an orbit.

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

iii). Finally, we show that any two irrationals \(\beta, \gamma\) 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 \(S \in \text{SL}(2, F_p)\) such that \(S(\beta) = \gamma\).

Taking the parallel transformation \((XY^2)^{-1} = YX: \beta \mapsto \beta + 1\) denoted by \(Z\). Since \(Z^n(\delta) = g\alpha\) for \(\delta = g\alpha + h\), put \(S(b\alpha) = d\alpha\). We obtain \(S(b\alpha) = d\alpha\) iff
\[S'(\alpha) = b^{-1}d\alpha \quad \text{for} \quad S = \begin{pmatrix} s & t \\ u & v \end{pmatrix}\]
and \(S' = \begin{pmatrix} b^{-1}sb \quad b^{-1}t \\ ub \quad v \end{pmatrix} \in \text{SL}(2, F_p)\).

Now it is enough to show that
\[S(\alpha) = \frac{s\alpha + t}{u\alpha + v} = d\alpha \quad \text{with} \quad sv - tu = 1
\]
for a suitable transformation \(S\), namely
\[\frac{(s\alpha + t)(u\alpha + v)}{(u\alpha + v)(u\alpha + v)} = \frac{su(-1) + su\alpha + tu(1 - \alpha) + tv}{u^2(-1) + uv + v^2} = \frac{u - su + tu + tv}{g(u, v)} = d\alpha\]
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 \(D_v = u^2 + 4\left(u^2 + d_0\right) = 5u^2 + 4d_0\) be the discriminant of the above quadratic equation on \(v\), then
iii). 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). We assume that \( d_0 \) is not square free in \( F_p \) for \( p \equiv 2, 3 \pmod{5} \). Assume that \( d_0 \) is not square free. Denoting a generator of the multiplicative group \( F_p^* \), namely a primitive root modulo \( p \) by \( r \).

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

If \( r^{2k+j+1} = r^{2k/r+1} \), namely \( 2k + 1 \equiv 2k + 1 \pmod{p-1} \), then \( r \equiv r^{2j} \pmod{p} \), hence \( 2j \equiv 2\ell \pmod{p-1} \), \( j = \ell \) holds for \( 0 \leq j - \ell \leq \frac{p-3}{2} \).

For \( m \left( 0 \leq m \leq \frac{p-3}{2} \right) \), 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.

By the transformation \( Z \cdot d_0^{(\alpha)\left(-su+ru+tv\right)} \) to \( S(\alpha) \), it was obtained \( ZS(\alpha) = d\alpha \), namely \( \alpha \) and \( d\alpha \) belongs to the same orbit. Therefore the following theorem was obtained.

**Theorem.** Let \( p \) be an odd prime and \( \alpha \) 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 \( F_p = \{ 0, 1, \ldots, p-1 \} \), 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 $F_p(\alpha) \setminus F_p$ of the length $p^2 - p$ by the action of $\text{PSL}(2, F_p)$; the details of these are presented in the diagram below:

![Diagram](attachment:image.png)

REFERENCES

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

