International Journal of Pure and Applied Mathematics
Volume 42 No. 4 2008, 549-554

EUCLIDEAN ALGORITHM MODULO 4 AND THE ROTATION GROUP $\boldsymbol{S_2 \times [3,4]^+}$

Toshihiro Watanabe
Department of Mathematical and Design Engineering
Gifu University
Yanagido, Gifu, 501-1193, JAPAN
e-mail: wata@gifu-u.ac.jp

Abstract: In Watanabe [4], the Euclidean algorithm modulo 4 is represented by the sequence of elements in the group $SL(2, \boldsymbol{F}_2)$ and the sum modulo 2 of values from the sequence. Watanabe [4] announced a new representation of the Jacobi symbol of quadratic residues by the sum modulo 2. This note gives a group structure of the sum modulo 2.

AMS Subject Classification: 11A55, 11A63
Key Words: Euclidean algorithm modulo 4, octahedral group

1. Introduction

The binary gcd algorithm gives interesting problems for the modular arithmetic in the binary number system (cf. Knuth [2]). As well-known, each coprime integers can be represented by the sequence of 2×2 matrices, that is the Euclidean algorithm. To calculate the sequence modulo 2^n gives a characterization of coprime integers until the n-bit. We call it the *Euclidean algorithm modulo* 2^n. In the case of modulo 4, Watanabe [4], which is for the combinatorics of quadratic residues, gives the representation by the sequence of elements in the group $SL(2, \boldsymbol{F}_2)$ and the sum modulo 2 of values from the sequence. In this note, the sum modulo 2 has the group structure, which is the direct product $\boldsymbol{S}_2 \times [3,4]^+$ of the permutation group $\boldsymbol{S}_2$ on two elements and the octahedral group $[3,4]^+$.

Received: August 17, 2007

2. Preliminaries

$< g_1, g_2, \cdots, g_r >$ is a group generated by the elements $g_1, g_2, \cdots, g_r$.

$\boldsymbol{F}_2$ is a field with two elements 0 and 1. In the finite vector 2-space $V(2, \boldsymbol{F}_2)$ over the field $\boldsymbol{F}_2$, the unit vectors are denoted by

$$\boldsymbol{e}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \boldsymbol{e}_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

The group $SL(2, \boldsymbol{F}_2)$ over the space $V(2, \boldsymbol{F}_2)$ is generated by

$$J_a = \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}, \quad a = 0, 1,$$

which satisfy the relation

$$J_0^2 = J_1^3 = (J_0 J_1)^2 = I \qquad (\mathrm{mod}\ 2),$$

where I is the identity of the group $SL(2, \boldsymbol{F}_2)$. For any {0,1}-sequence $a_n a_{n-1} \cdots a_1$, set

$$g_n^{(k)} = J_{a_n} J_{a_{n-1}} \cdots J_{a_1} g_0^{(k)}, \quad k = 0, 1, \infty,$$

where $g_0^{(0)} = I, g_0^{(1)} = J_1$ and $g_0^{(\infty)} = J_0$.

Thus the sequence $a_n a_{n-1} \cdots a_1$ gives *three random walks* on the Cayley diagram of $SL(2, \boldsymbol{F}_2)$ starting at $g_0^{(k)}, k = 0, 1, \infty$. For each random walk, let us consider the following:

$$\Lambda(g_n^{(k)}) = \begin{pmatrix} \sum_{\substack{g_m^{(k)} = g_0^{(\infty)^{-1}} \\ 1 \le m \le n}} a_m \\ \sum_{\substack{g_m^{(k)} = g_0^{(1)^{-1}} \\ 1 \le m \le n}} a_m \end{pmatrix}, \quad k = 0, 1, \infty, \tag{1}$$

where $g_m^{(k)} = J_{a_m} J_{a_{m-1}} \ldots J_{a_1} g_0^{(k)}$.

Remark 1. Watanabe [4] uses the vector of binary letters ${}^t(a_i, b_i)$ from the coefficients modulo 4 of the Euclidean algorithm. But we can easily see that the letter ${}^t(a, 1)$ in the algorithm is transformed into a word of letters ${}^t(a', 0)$, for example:

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

Therefore Λ_n of Proposition 9.2.1 in [4], can be replaced by $\Lambda(g_n^{(k)}), k = 0, 1, \infty$, and the same proposition holds.

We note the easy and useful properties as follows:

(i) The six elements $g_0^{(\infty)^{-1}} g_0^{(k)^{-1}}$ and $g_0^{(1)^{-1}} g_0^{(k)^{-1}}, k = 0, 1, \infty$ are different

from each other and give all elements in $SL(2, \boldsymbol{F}_2)$. Then each entry of the vectors $\Lambda(g_n^{(k)}), k = 0, 1, \infty$ puts the sequence $a_n a_{n-1} a_{n-2} \cdots a_1$ into the sum modulo 2 of values a_i across the above corresponding element in the path from I to $J_{a_n} J_{a_{n-1}} J_{a_{n-2}} \cdots J_{a_1}$, respectively.

(ii) For any $g \in SL(2, \boldsymbol{F}_2)$, the elements $g g_0^{(i)}$, $i = 0, 1, \infty$ are in each different coset $g_0^{(i')} < J_1 J_0 >, i' = 0, 1, \infty$, respectively. The subgroup $< J_1 J_0 >$ has only two elements.

3. Group Property of $\Lambda(g_n^{(k)})$, $k = 0, 1, \infty$

This is the main issue in this note.

From (ii) of Section 2, set $(i_m; p_m), (j_m; q_m)$ and $(k_m; r_m)$ in $\{0, 1, \infty\} \times \boldsymbol{F}_2, m = 0, 1, \cdots, n-1$ to satisfy

$$g_{n-m}^{(i_m)} = g_0^{(0)} (J_1 J_0)^{p_m}, \quad g_{n-m}^{(j_m)} = g_0^{(1)} (J_1 J_0)^{q_m}, \quad g_{n-m}^{(k_m)} = g_0^{(\infty)} (J_1 J_0)^{r_m}. \quad (2)$$

Set

$$\Lambda(g_{n-m}^{(i_m)}) = \Lambda(i_m; p_m), \quad \Lambda(g_{n-m}^{(j_m)}) = \Lambda(j_m; q_m), \quad \Lambda(g_{n-m}^{(k_m)}) = \Lambda(k_m; r_m).$$

Let us, for each g_{n-m}, consider the following triplet ordered by (2):

$$(\Lambda(i_m; p_m), \Lambda(j_m; q_m), \Lambda(k_m; r_m)).$$

We have for $a_{n-m} = 1$,

$$\begin{aligned} g_{n-m-1}^{(i_{m+1})} &= J_1^{-1} g_{n-m}^{(j_m)} = g_0^{(0)} (J_1 J_0)^{q_m}; \\ g_{n-m-1}^{(j_{m+1})} &= J_1^{-1} g_{n-m}^{(k_m)} = g_0^{(1)} (J_1 J_0)^{r_m+1}; \\ g_{n-m-1}^{(k_{m+1})} &= J_1^{-1} g_{n-m}^{(i_m)} = g_0^{(\infty)} (J_1 J_0)^{p_m+1} \end{aligned}$$

and for $a_{n-m} = 0$,

$$\begin{aligned} g_{n-m-1}^{(i_{m+1})} &= J_0^{-1} g_{n-m}^{(k_m)} = g_0^{(0)} (J_1 J_0)^{r_m}; \\ g_{n-m-1}^{(j_{m+1})} &= J_0^{-1} g_{n-m}^{(j_m)} = g_0^{(1)} (J_1 J_0)^{q_m+1}; \\ g_{n-m-1}^{(k_{m+1})} &= J_0^{-1} g_{n-m}^{(i_m)} = g_0^{(\infty)} (J_1 J_0)^{p_m}. \end{aligned}$$

Using the *not* operation on $\boldsymbol{F}_2$

$$\bar{a} = \begin{cases} 1 & \text{if } a = 0, \\ 0 & \text{if } a = 1, \end{cases}$$

we obtain

$$\begin{aligned} &(\Lambda(i_{m+1}; p_{m+1}), \Lambda(j_{m+1}; q_{m+1}), \Lambda(k_{m+1}; r_{m+1})) \\ &= \begin{cases} (\Lambda(k_m; r_m), \Lambda(j_m; \bar{q}_m), \Lambda(i_m; p_m)), & \text{for } a_{n-m} = 0, \\ (\Lambda(j_m; q_m), \Lambda(k_m; \bar{r}_m) + \boldsymbol{e}_{r_m}, \Lambda(i_m; \bar{p}_m)), & \text{for } a_{n-m} = 1. \end{cases} \end{aligned} \quad (3)$$

The above transformation (3) is denoted by

$$(\Lambda(i_{m+1};p_{m+1}),\Lambda(j_{m+1};q_{m+1}),\Lambda(k_{m+1},r_{m+1})) \\ = S_{a_{n-m}}\left(\Lambda(i_m;p_m),\Lambda(j_m;q_m),\Lambda(k_m;r_m)\right). \quad (4)$$

Thus we have

$$S_{a_1}S_{a_2}\cdots S_{a_n}\left(\Lambda(i_0;p_0),\Lambda(j_0;q_0),\Lambda(k_0;r_0)\right)=(\mathbf{0},\mathbf{0},\mathbf{0}),\quad \mathbf{0}={}^t(0,0). \quad (5)$$

We call the triplet (p_0,q_0,r_0) the *initial state* and (p_m,q_m,r_m) the *m-th state* of (5).

Now let us investigate into the group property of the transformations $S_a, a=0,1$. We note the ordering (2) is given by the transformations $S_a, a=0,1$ and the *initial triplet* of (5)

$$(\Lambda(i_0;p_0),\Lambda(j_0;q_0),\Lambda(k_0;r_0)).$$

Thus for any given $(p_0,q_0,r_0)\in \boldsymbol{F}_2\times\boldsymbol{F}_2\times\boldsymbol{F}_2$, set any *initial ordered triplet* as follows:

$$((\boldsymbol{c}_0;p_0),(\boldsymbol{c}_1;q_0),(\boldsymbol{c}_\infty;r_0)),\quad \boldsymbol{c}_k\in V(2,\boldsymbol{F}_2),\ k=0,1,\infty.$$

In (5),

$$\boldsymbol{c}_0=\Lambda(i_0;p_0),\quad \boldsymbol{c}_1=\Lambda(j_0;q_0),\quad \boldsymbol{c}_\infty=\Lambda(k_0;r_0).$$

Let us consider triplets ordered with the initial ordered triplet and the following transformations τ_1,τ_2,R,P. Set thus *ordered triplet*

$$((\boldsymbol{x}_0;s_0),(\boldsymbol{x}_1;s_1),(\boldsymbol{x}_\infty;s_\infty)),\quad \boldsymbol{x}_k\in V(2,\boldsymbol{F}_2), s_k\in\boldsymbol{F}_2, k=0,1,\infty.$$

Define the transformations τ_1 and τ_2 on the ordered triplets:

$$\begin{aligned}\tau_1((\boldsymbol{x}_0;s_0),(\boldsymbol{x}_1;s_1),(\boldsymbol{x}_\infty;s_\infty)) &= ((\boldsymbol{x}_1;s_1),(\boldsymbol{x}_0;s_0),(\boldsymbol{x}_\infty;s_\infty));\\ \tau_2((\boldsymbol{x}_0;s_0),(\boldsymbol{x}_1;s_1),(\boldsymbol{x}_\infty;s_\infty)) &= ((\boldsymbol{x}_\infty;s_\infty),(\boldsymbol{x}_1;s_1),(\boldsymbol{x}_0;s_0)).\end{aligned}$$

The transformations R and P operate only on the state (s_0,s_1,s_∞):

$$\begin{aligned}R((\boldsymbol{x}_0;s_0),(\boldsymbol{x}_1;s_1),(\boldsymbol{x}_\infty;s_\infty)) &= ((\boldsymbol{x}_0;\bar{s}_0),(\boldsymbol{x}_1;s_1),(\boldsymbol{x}_\infty;s_\infty));\\ P((\boldsymbol{x}_0;s_0),(\boldsymbol{x}_1;s_1),(\boldsymbol{x}_\infty;s_\infty)) &= ((\boldsymbol{x}_0+\boldsymbol{e}_{s_o};s_0),(\boldsymbol{x}_1;s_1),(\boldsymbol{x}_\infty;s_\infty)).\end{aligned}$$

We note the following properties:

$$\begin{aligned}R^{\tau_1}((\boldsymbol{x}_0;s_0),(\boldsymbol{x}_1;s_1),(\boldsymbol{x}_\infty;s_\infty)) &= ((\boldsymbol{x}_0;s_0),(\boldsymbol{x}_1;\bar{s}_1),(\boldsymbol{x}_\infty;s_\infty));\\ R^{\tau_2}((\boldsymbol{x}_0;s_0),(\boldsymbol{x}_1;s_1),(\boldsymbol{x}_\infty;s_\infty)) &= ((\boldsymbol{x}_0;s_0),(\boldsymbol{x}_1;s_1),(\boldsymbol{x}_\infty;\bar{s}_\infty));\\ P^{\tau_1}((\boldsymbol{x}_0;s_0),(\boldsymbol{x}_1;s_1),(\boldsymbol{x}_\infty;s_\infty)) &= ((\boldsymbol{x}_0;s_0),(\boldsymbol{x}_1+\boldsymbol{e}_{s_1};s_1),(\boldsymbol{x}_\infty;s_\infty));\\ P^{\tau_2}((\boldsymbol{x}_0;s_0),(\boldsymbol{x}_1;s_1),(\boldsymbol{x}_\infty;s_\infty)) &= ((\boldsymbol{x}_0;s_0),(\boldsymbol{x}_1;s_1),(\boldsymbol{x}_\infty+\boldsymbol{e}_{s_\infty};s_\infty))\end{aligned}$$

and for $i \neq j,\ i,j \in \{1,2\}$

$$\begin{array}{lllllll} PR^{\tau_i} & = & R^{\tau_i}P, & RP^{\tau_i} & = & P^{\tau_i}R, & R^{\tau_i}P^{\tau_j} = P^{\tau_j}R^{\tau_i}\,, \\ RR^{\tau_i} & = & R^{\tau_i}R, & PP^{\tau_i} & = & P^{\tau_i}P\,, & \\ P^{\tau_i}\tau_j & = & \tau_j P^{\tau_i}, & R^{\tau_i}\tau_j & = & \tau_j R^{\tau_i}, & \end{array}$$

where $g^h = h^{-1}gh$.

Remark 2. (i) The subgroup $< \tau_1, \tau_2 >$ is the permutation group $\boldsymbol{S}_3$ on three elements. The subgroup $< R >$ is the permutation group $\boldsymbol{S}_2$ on two elements. The subgroup $< R, \tau_1, \tau_2 >$ is the wreath product $\boldsymbol{S}_2 \wr \boldsymbol{S}_3$ (cf. Rotman [3]).

(ii) The transformation P *produces* or *removes* the vectors $\boldsymbol{e}_i, i = 0, 1$ depending only on the state (s_0, s_1, s_∞).

Thus S_0 and S_1 become transformations on ordered triplets and

$$S_0 = \tau_2 R^{\tau_1}, \quad S_1 = \tau_1\tau_2 R(RP)^{\tau_2}.$$

Then we have the following *main result* to characterize the transformations S_0 and S_1.

Proposition. *For the transformations S_0 and S_1 with any fixed initial ordered triplet, the following relations hold:*

$$S_0^2 = S_1^6 = (S_0S_1)^4 = E\,, \tag{6}$$

$$(S_0S_1^3)^2 = (PR)^2((PR)^2)^{\tau_1}((PR)^2)^{\tau_2}\,, \tag{7}$$

where E is the identity.

Proof. We have the following:

$$\begin{aligned} S_0^2 &= \tau_2 R^{\tau_1} \cdot \tau_2 R^{\tau_1} = E; \\ S_1^3 &= \tau_1\tau_2 R\underline{(RP)^{\tau_2} \cdot \tau_1\tau_2} R\underline{(RP)^{\tau_2} \cdot \tau_1\tau_2} R(RP)^{\tau_2} \\ &= \tau_1\tau_2 R\tau_1\tau_2\underline{RPR\tau_1}\tau_2 RPR(RP)^{\tau_2} \\ &= \tau_1\tau_2 R\underline{\tau_1\tau_2\tau_1}(RPR)^{\tau_1}\tau_2(RPR)(RP)^{\tau_2} \\ &= \underline{\tau_1\tau_2 R\tau_2\tau_1}\underline{\tau_2}(RPR)^{\tau_1}\underline{\tau_2}(RPR)(RP)^{\tau_2} \\ &= R^{\tau_2}(RPR)^{\tau_1}(RPR)(RP)^{\tau_2} = (RPR)(RPR)^{\tau_1}P^{\tau_2}; \\ (S_0S_1^3)^2 &= \tau_2 R^{\tau_1} \cdot (RPR)\underline{(RPR)^{\tau_1}P^{\tau_2} \cdot \tau_2} R^{\tau_1} \cdot (RPR)(RPR)^{\tau_1}P^{\tau_2} \\ &= \underline{\tau_2 R^{\tau_1}(RPR)\tau_2}(RPR)^{\tau_1}PR^{\tau_1}(RPR)(RPR)^{\tau_1}P^{\tau_2} \\ &= \underline{R^{\tau_1}(RPR)^{\tau_2}(RPR)^{\tau_1}}P\underline{R^{\tau_1}(RPR)(RPR)^{\tau_1}}P^{\tau_2} \\ &= (PR)^{\tau_1}(RPR)^{\tau_2}(PR)^2(PR)^{\tau_1}P^{\tau_2} = (PR)^2((PR)^2)^{\tau_1}((PR)^2)^{\tau_2}; \\ S_0S_1 &= \tau_2\underline{R^{\tau_1} \cdot \tau_1\tau_2 R(RP)^{\tau_2}} = \tau_2\tau_1\underline{RR^{\tau_2}}RP\tau_2 \end{aligned}$$

$$= \tau_2\tau_1\underline{R^{\tau_2}P}\tau_2 = \tau_2\tau_1\tau_2 RP^{\tau_2};$$
$$(S_0S_1)^2 = \tau_2\tau_1\underline{\tau_2 RP^{\tau_2}\cdot\tau_2}\tau_1\underline{\tau_2 RP^{\tau_2}} = \tau_2\underline{\tau_1 R^{\tau_2}P\tau_1}R^{\tau_2}P\tau_2$$
$$= \tau_2\underline{\tau_1 R^{\tau_2}\tau_1}P^{\tau_1}R^{\tau_2}P\tau_2 = \tau_2 R^{\tau_2}P^{\tau_1}R^{\tau_2}P\tau_2 = P^{\tau_1}P^{\tau_2}.$$

In the above computation, the elements with the underline are transformed. Thus we obtain the relations (6) and (7). □

Remark 3. Since from the above proof,

$$(\tau_2 R^{\tau_1})^2 = (\tau_1\tau_2 RR^{\tau_2})^3 = (\tau_2 R^{\tau_1}\cdot\tau_1\tau_2 RR^{\tau_2})^2 = E,$$

the group $< \tau_2 R^{\tau_1}, \tau_1\tau_2 RR^{\tau_2} >$ is the subgroup $\boldsymbol{S}_3$ in the group $\boldsymbol{S}_2 \wr \boldsymbol{S}_3$.

Since the element $(PR)^2((PR)^2)^{\tau_1}((PR)^2)^{\tau_2}$ is in the center of the group $\langle S_0, S_1\rangle$, the quotient group $\langle S_0, S_1\rangle / \left\langle (PR)^2((PR)^2)^{\tau_1}((PR)^2)^{\tau_2}\right\rangle$ has the relation

$$S_0^2 = S_1^6 = (S_0S_1)^4 = (S_0S_1^3)^2 = E. \tag{8}$$

By Coxeter and Moser [1], the group defined by the relation (8) is the direct product

$$\boldsymbol{S}_2 \times [3,4]^+$$

of the group $\boldsymbol{S}_2$ generated by S_1^3 and the octahedral group $[3,4]^+$ generated by S_1^4 and $S_0S_1^3$.

Therefore we obtain from (5) as follows:

$$(\Lambda(i_0;p_0), \Lambda(j_0;q_0), \Lambda(k_0;r_0)) = S_{a_n}^{-1}S_{a_{n-1}}^{-1}\cdots S_{a_1}^{-1}(\mathbf{0},\mathbf{0},\mathbf{0}). \tag{9}$$

References

[1] H.S.M. Coxeter, W.O. Moser, *Generators and Relations for Discrete Groups*, 3-th Edition, Springer, Berlin (1972), 116.

[2] D.E. Knuth, *The Art of Computer Programming*, Chapter 4, Volume 2, Addison-Wesley, Reading (1981).

[3] J.J. Rotman, *An Introduction to the Theory of Groups*, 4-th Edition, Graduate Texts in Mathematics, **148**, Springer, Berlin (1994), 175.

[4] T. Watanabe, Random walks on $SL(2, F_2)$ and Jacobi symbols of quadratic residues, In: *Advances in Combinatorial Methods and Applications to Probability and Statistics* (Ed. N. Balakrishnan), Statistics in Industry and Technology Series, Birkhäuser, Boston (1997), 125-134.