On some properties of 2×2 integral matrices

Takeo FUNAKURA

Department of General Education, Okayama University of Science
Ridai-cho, Okayama 700, Japan

Nobuaki MORIMOTO, Masao TOYOIZUMI, Noriaki KAMIYA

Department of Mathematics, Rikkyo University
Nishi-Ikebukuro, Toshima-ku, Tokyo 171, Japan

(Received September 21, 1979)

Synopsis: Professor T. Mitsui set the problem of finding conditions that a square matrix with integral entries is a quadratic residue modulo a prime. We solve this problem in the case of order 2 and further consider some related topics.

0. Introduction

Throughout this paper, the number p always denotes an odd prime. Denote by $M(n, \mathbf{Z})$ the ring of $n\times n$ matrices with integral entries. Let A be a matrix in $M(n, \mathbf{Z})$ such that $A\not\equiv O(\mathrm{mod}\ p)$. A is called a quadratic residue modulo p if there exists a matrix X in $M(n, \mathbf{Z})$ such that $X^2\equiv A\ (\mathrm{mod}\ p)$. A is called a quadratic non-residue modulo p if there exists no such X. At the informal meeting of number theory held at the Gakushuin University in 1977, Professor T. Mitsui set the problem of finding conditions that A is a quadratic residue modulo p. In the first section 1, we shall solve this problem in the matrix ring $M(2, \mathbf{Z})$.

Now, let $\mathbf{F}_p$ denote the finite field of order p. Define three sets R, $R^\times$ and $SO(2)$ as follows:

$$R=\left\{\begin{pmatrix} a & b\\ -b & a\end{pmatrix} \mid a,\ b\in\mathbf{F}_p\right\},$$

$$R^\times=\{Y\in R\mid \det Y\neq 0\}$$

and

$$SO(2)=\{Y\in R^\times\mid \det Y=1\}.$$

Then it is easy to see that R is a commutative ring and $R^\times$ is a commutative group containing $SO(2)$ as a subgroup. In the last section 2, we shall prove some properties of these sets.

The following additional notation will be used in this paper. For any integer

a, we define the symbol $\chi(a)$ by the relations

$$\chi(a)=\begin{cases}\left(\frac{a}{p}\right) & \text{if } a\not\equiv 0 \pmod{p},\\ 0 & \text{if } a\equiv 0 \pmod{p},\end{cases}$$

where $\left(\frac{a}{p}\right)$ is the Legendre symbol. As usual, $\mathbf{Z}$ will denote the ring of rational integers. Denote by $M(2, \mathbf{F}_p)$ the 2×2 matrix ring over $\mathbf{F}_p$. Furthermore, if S is a set, we write $|S|$ for the cardinal number of S.

1. Mitsui's problem in $M(2, \mathbf{Z})$

THEOREM 1. *Let A be a matrix of order 2 with integral entries. Then A is a quadratic residue modulo p if and only if A satisfies* (I) *and one of* (II) *in the following statements.*

(I) $\chi(\det A)=0$ *or* 1.

This implies that the congruence $X^2\equiv \det A \pmod{p}$ has integer solutions. In the following, k will denote a root of this congruence.

(II) (i) $\chi(\operatorname{tr} A+2k)=1$.

(ii) $\chi(\operatorname{tr} A-2k)=1$.

(iii) $A\equiv \pm\begin{pmatrix}k & 0\\ 0 & k\end{pmatrix} \pmod{p}$.

PROOF. Put $A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$. Clearly, A is a quadratic residue modulo p if and only if the simultaneous congruences

$$(*)\qquad \begin{aligned} x^2+yz &\equiv a && (1)\\ (x+w)y &\equiv b && (2)\\ (x+w)z &\equiv c && (3)\\ w^2+yz &\equiv d && (4)\end{aligned} \pmod{p}$$

have integer solutions.

Now, let us suppose that there exist integers x, y, z, w satisfying the congruences (*). Then we can easily show that

$$(xw-yz)^2\equiv \det A \pmod{p},$$

which implies $\chi(\det A)=0$ or 1. Hence, we know that

$$xw-yz\equiv \pm k \pmod{p}.$$

In the case $xw-yz\equiv k \pmod{p}$, we obtain from (1) and (4),

$$a+d+2k\equiv (x+w)^2,$$

and so

$$\operatorname{tr} A+2k\equiv (x+w)^2 \pmod{p}. \qquad (5)$$

If $\operatorname{tr} A+2k\not\equiv 0 \pmod{p}$, then we have $\chi(\operatorname{tr} A+2k)=1$.

If $\mathrm{tr}\, A+2k\equiv 0 \pmod p$, then from (5), we get

$$x+w\equiv 0 \pmod p.$$

Therefore, from (1), (2), (3) and (4), we find that

$$a\equiv d\equiv -k \text{ and } b\equiv c\equiv 0 \pmod p,$$

which imply

$$A\equiv\begin{pmatrix}-k & 0\\ 0 & -k\end{pmatrix} \pmod p.$$

In the case $xw-yz\equiv -k \pmod p$, we obtain

$$\chi(\mathrm{tr}\, A-2k)=1 \text{ or } A\equiv\begin{pmatrix}k & 0\\ 0 & k\end{pmatrix} \pmod p$$

as can be seen by using the same way as above.

Conversely, let us suppose that the conditions (I) and (i) of (II) are fulfilled. Then there exists an integer m such that $m^2\equiv a+d+2k$ and $m\not\equiv 0 \pmod p$. So we can find an integer n such that $mn\equiv 1 \pmod p$. We put

$$x=n(a+k),\ y=nb,\ z=nc \text{ and } w=m-n(a+k),$$

which satisfy the simultaneous congruences (*). The proof of other cases are similar to that of the above, and we omit them.

2. Some properties of R, R' and $SO(2)$

LEMMA 1.
$$|R'|=\begin{cases} p^2-1 & \text{if } p\equiv 3 \pmod 4,\\ (p-1)^2 & \text{if } p\equiv 1 \pmod 4.\end{cases}$$

PROOF. Let i denote a root of the equation $x^2+1=0$ in the algebraic closed field of $\mathbf{F}_p$. Then i belongs to $\mathbf{F}_{p^2}$, where $\mathbf{F}_{p^2}$ is the finite field of order p^2. We define a homomorphism

$$\varphi : R' \longrightarrow \mathbf{F}_{p^2}^{\times}$$

by the relation

$$\varphi\left(\begin{pmatrix}a & b\\ -b & a\end{pmatrix}\right)=a+bi.$$

If $p\equiv 3 \pmod 4$, then i do not lie in $\mathbf{F}_p$, so that φ is an isomorphism. Therefore, we get $|R'|=p^2-1$.

If $p\equiv 1 \pmod 4$, then i is in $\mathbf{F}_p$. Thus the number of (a, b) satisfying the equation

$$a^2+b^2=0,$$
$$a,\ b\in\mathbf{F}_p$$

is $2p-1$. So we have $|R'|=p^2-(2p-1)=(p-1)^2$.

LEMMA 2. $$|SO(2)|=p-\left(\frac{-1}{p}\right).$$

PROOF. In the following, we identify $\mathbf{F}_p$ with $\mathbf{Z}/p\mathbf{Z}$ and naturally regard χ

as a function on $\mathbf{F}_p$.

Clearly,

$$\begin{aligned}\sum_{a\in\mathbf{F}_p}\chi(1-a^2) &= \sum_{a\in\mathbf{F}_p}\chi(1+a)\chi(1-a)\\ &= \sum_{\substack{a\in\mathbf{F}_p\\ a\neq -1}}\chi\left(\frac{1-a}{1+a}\right)\\ &= \sum_{\substack{b\in\mathbf{F}_p\\ b\neq -1}}\chi(b)\\ &= -\chi(-1)\\ &= -\left(\frac{-1}{p}\right).\end{aligned}$$

On the other hand, we know that

$$\sum_{a\in\mathbf{F}_p}|\chi(1-a^2)| = p-2.$$

Hence, from the definition of $SO(2)$, we obtain

$$\begin{aligned}|SO(2)| &= 2\sum_{\substack{a\in\mathbf{F}_p\\ \chi(1-a^2)=1}}1+2\\ &= \sum_{a\in\mathbf{F}_p}\{\chi(1-a^2)+|\chi(1-a^2)|\}+2\\ &= p-\left(\frac{-1}{p}\right).\end{aligned}$$

PROPOSITION. (1) *If* $p\equiv 3 \pmod 4$, *we have*

$$R\cong\mathbf{F}_{p^2},$$

$$R^\times\cong\mathbf{F}_{p^2}{}^\times$$

and $R^\times/SO(2)\cong\mathbf{F}_p{}^\times$.

(2) *If* $p\equiv 1 \pmod 4$, *we have*

$$R^\times\cong\mathbf{F}_p{}^\times\times\mathbf{F}_p{}^\times$$

and $SO(2)\cong\mathbf{F}_p{}^\times$.

PROOF. Assume that $p\equiv 3 \pmod 4$. Then $R^\times\cong\mathbf{F}_{p^2}{}^\times$ as we have seen in the proof of Lemma 1. Since $a^2+b^2=0$ and $a, b\in\mathbf{F}_p$ imply $a=b=0$, we have $R\cong\mathbf{F}_{p^2}$. Noticing that $|R^\times/SO(2)|=p-1$ by Lemmas 1 and 2, we can easily deduce $R^\times/SO(2)\cong\mathbf{F}_p{}^\times$.

Now assume that $p\equiv 1 \pmod 4$. Let φ be the homomorphism defined in Lemma 1. Then the restriction of φ gives a homomorphism from $SO(2)$ to $\mathbf{F}_p{}^\times$. It is easily verified that this is an isomorphism. Since $|R^\times/SO(2)|=p-1$, we readily find that $R^\times/SO(2)\cong\mathbf{F}_p{}^\times$.

Putting

$$\begin{pmatrix} a & b\\ -b & a\end{pmatrix}^n=\begin{pmatrix} a_n & b_n\\ -b_n & a_n\end{pmatrix},$$

we obtain

$$a_n=\sum_{0\leq 2k\leq n}\binom{n}{2k}(-1)^k a^{n-2k}b^{2k}$$

and

$$b_n=\sum_{1\leq 2k+1\leq n}\binom{n}{2k+1}(-1)^k a^{n-2k-1}b^{2k+1},$$

which yield

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}^p=\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

If $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ belongs to $R^\times$, then we get

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}^{p-1}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Thus the order of any element of $R^\times$ divides $p-1$. By the fact that $R^\times/SO(2)\cong\mathbf{F}_p^\times$, we see that $R^\times/SO(2)$ is a cyclic group of order $p-1$. Hence, there exists an element A in $R^\times$ such that $R^\times=\langle A\rangle\cdot SO(2)$, where $\langle A\rangle$ denotes the cyclic group generated by A. Here we note that $A^{p-1}\in SO(2)$ and $A^m\notin SO(2)$ for any positive integer $m<p-1$. Therefore, we know that $A^{p-1}=1_2$, where 1_2 is a unit matrix, and $R^\times=\langle A\rangle\times SO(2)$. Since $\langle A\rangle\cong\mathbf{F}_p^\times\cong SO(2)$, we obtain $R^\times=\mathbf{F}_p^\times\times\mathbf{F}_p^\times$.

Thus we have completed the proof.

LEMMA 3. (1) *If* $p\equiv 3 \pmod 4$, *we have*

$$SO(2)=\left\{\begin{pmatrix} \dfrac{t^2-1}{t^2+1} & \dfrac{2t}{t^2+1} \\ -\dfrac{2t}{t^2+1} & \dfrac{t^2-1}{t^2+1} \end{pmatrix}\ t\in\mathbf{F}_p\right\}\cup\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\}$$

(2) *If* $p\equiv 1 \pmod 4$, *we have*

$$SO(2)=\left\{\begin{pmatrix} \dfrac{t^2+1}{2t} & \dfrac{t^2-1}{2ti} \\ -\dfrac{t^2-1}{2ti} & \dfrac{t^2+1}{2t} \end{pmatrix}\ t\in\mathbf{F}_p^\times\right\},$$

where i *is a root of the equation* $x^2+1=0$ *in* the algebraic closed field of $\mathbf{F}_p$.

The proof is easy and will be omitted.

Now, if $A\in M(2, \mathbf{Z})$, we shall denote by A^* the matrix defined by

$$A^*=A \pmod p,$$

which belongs to $M(2, \mathbf{F}_p)$, since we identify $\mathbf{F}_p$ with $\mathbf{Z}/p\mathbf{Z}$.

THEOREM 2. *Let* A *be a* 2×2 *integral matrix, and suppose* A^* *lies in* $SO(2)$. *Then the following assertions hold.*

(1) *If* $p\equiv 3 \pmod 4$, *then* A *is a quadratic residue modulo* p.

(2) *If* $p\equiv 1 \pmod 4$, *then* A *is a quadratic residue modulo* p *if and only if*

$\chi(t)=1$, *where* t *is an element in* $\mathbf{F}_p^\times$ *which corresponds to* A^* *in the sense of Lemma* 3.

PROOF. (1) From Lemma 3, we obtain

$$\begin{aligned}\chi(\mathrm{tr}\ A^*-2)&=\chi\left(\frac{-4}{t^2+1}\right)\\&=\chi(-1)\chi(t^2+1)\\&=-\chi(t^2+1),\end{aligned}$$

where t is an element in $\mathbf{F}_p$. If $t\neq 0$, namely, $A^*\neq -1_2$, we get

$$\begin{aligned}\chi(\mathrm{tr}\ A^*+2)&=\chi\left(\frac{4t^2}{t^2+1}\right)\\&=\chi(t^2+1).\end{aligned}$$

Thus our assertion follows immediately from Theorem 1 unless $A^*=-1_2$. But, when $A^*=-1_2$, our assertion also holds.

(2) The proof is similar to the one of (1), and we omit it.

Takeo FUNAKURA
Department of General Education, Okayama University of Science
Ridai-cho, Okayama, Japan,

Nobuaki MORIMOTO, Masao TOYOIZUMI, Noriaki KAMIYA
Department of Mathematics, Rikkyo University
Nishi-Ikebukuro, Tokyo, Japan