ON INTEGER ROOTS OF THE UNIT MATRIX.†

By R. P. BAMBAH *and* S. CHOWLA.

(Communicated by Sir S. S. Bhatnagar, F.R.S.)

(*Read January 17, 1947.*)

§1. The study of Vaidyanathaswamy's paper (1928) has led us to conjecture that:

If p denotes a prime, all the integer matrices X_{p-1} of order $(p-1)$, except E_{p-1} itself, such that

$$[X_{p-1}]^p = E_{p-1}$$

where E_{p-1} is the unit matrix of order $(p-1)$, can be expresed as

$$\Delta^{-1} M_{p-1} \Delta$$

[i.e. transform of M_{p-1} by Δ] where Δ is an integer matrix of order $(p-1)$ and determinant ± 1, and

$$M_{p-1} = \begin{bmatrix} -1 & -1 & . & . & -1 & -1 \\ 1 & 0 & . & . & 0 & 0 \\ 0 & 1 & . & . & 0 & 0 \\ . & . & . & . & . & . \\ 0 & 0 & . & . & 1 & 0 \end{bmatrix}$$

(I) In this paper we prove this conjecture for $p = 3$.

§2. In this section we prove that
the necessary and sufficient conditions for the integer matrix

$$X_2 = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \neq E_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

to be a cube root of E_2 are

(II) $$a+d = -1 \quad \text{and} \quad ad-bc = 1.$$

Consider the transformation

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}(x, y) = ax+by,\ cx+dy.$$

It can be easily verified that

$$A^3 = (a^3+2abc+bcd)x+b(a^2+ad+d^2+bc)y,$$
$$c(a^2+ad+d^2+bc)x+(d^3+2bcd+bca)y.$$

Therefore the necessary and sufficient conditions for X_2 to be a cube root of E_2 are (except when $X_2 = E_2$)

$$a^3+2abc+bcd = 1 \qquad \text{(i)}$$
$$a^2+ad+d^2+bc = 0 \qquad \text{(ii)}$$
$$d^3+2bcd+bca = 1 \qquad \text{(iii)}$$

---

† All letters in this paper denote integers.

It can be easily seen that

$$(iii) = (i)+(d-a)(ii).$$

Therefore we obtain the necessary and sufficient conditions as

$$a^3+(2a+d)bc = 1 \qquad (i)$$
$$a^2+ad+d^2+(bc) = 0 \qquad (ii)$$

Eliminating bc from these equations we have

$$(a+d)^3 = -1 \quad \text{or} \quad (a+d) = -1$$

as a necessary condition.
Also from (ii) we have

$$bc = -(a^2+ad+d^2) = ad-(a+d)^2$$
$$= ad-1.$$

Hence $ad-bc = 1$, is another necessary condition.

That these two conditions are sufficient can be easily verified with the help of (i) and (ii).

§3. On account of (II) the proof of (I) reduces to showing that

$$X_2 = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

where $a+d = -1$ and $ad-bc = 1$, can be expressed as

$$\Delta^{-1} M_2 \Delta$$

where

$$\Delta = \begin{bmatrix} A & B \\ C & D \end{bmatrix}, \quad AD-BC = \pm 1$$

and

$$M_2 = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}.$$

This we shall prove in this section.

We shall consider only the case when b is negative. The case when b is positive can be similarly treated by taking Δ of determinant -1. That b cannot be zero can be easily seen.

We can easily prove the following lemmas:

(1) If $\Delta = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ and $AD-BC = 1$,

$$\Delta^{-1} = \begin{bmatrix} D & -B \\ -C & A \end{bmatrix}.$$

(2) $$\Delta^{-1} M_2 \Delta = \begin{bmatrix} -CD-AD-AB & -D^2-BD-B^2 \\ C^2+AC+A^2 & CD+BC+AB \end{bmatrix}.$$

Now

$$ad-bc = 1;$$

therefore

$$-bc = 1-ad = 1-a(-a-1)$$
$$= a^2+a+1.$$

It is well known that all factors of a^2+a+1 are of the form k^2+l^2+kl.

We choose A, B, C and D such that

$$-b = D^2+BD+B^2 \tag{iv}$$

$$c = C^2+AC+A^2 \tag{v}$$

and

$$AD-BC = 1 \tag{vi}$$

That A, B, C and D can be chosen to satisfy (vi) will be proved in §4.

Now we shall show that

$$a = -CD-AD-AB \tag{vii}$$

and

$$d = CD+BC+AB \tag{viii}$$

As

$$a^2+a+1 = -bc = (B^2+D^2+BD)(A^2+C^2+AC),$$

we have

$$a^2+a+[1-(B^2+D^2+BD)(A^2+C^2+AC)] = 0.$$

The roots of this equation in a are

$$-CD-AD-AB \quad \text{and} \quad CD+BC+AB,$$

for

$$\begin{aligned}(-CD-AD-AB)+(CD+BC+AB) &= -(AD-BC)\\ &= -1\end{aligned}$$

and

$$\begin{aligned}&\{(-CD-AD-AB)(CD+BC+AB)\}\\ &-[1-(B^2+D^2+BD)(A^2+C^2+AC)]\\ &= -1+(AD-BC)^2 = 0.\end{aligned}$$

We, therefore, have

$$a = (-CD-AD-AB) \quad \text{or} \quad (CD+BC+AB).$$

In case a has the second value, replace A, C, B and D by C, A, $-D$ and $-B$ respectively. Obviously (iv), (v) and (vi) are unaffected while a has the value $-CD-AD-AB$.

So that in all cases we have

$$a = -CD-AD-AB$$

and hence

$$\begin{aligned}d = -1-a &= -1+CD+AD+AB\\ &= CD+BC+AB.\end{aligned}$$

From (iv), (v), (vi), (vii) and (viii) it follows that we can choose A, B, C and D to satisfy

$$X_2 = \Delta^{-1}M_2\Delta$$

where

$$\Delta = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \quad \text{and} \quad AD-BC = 1.$$

§4.

THEOREM:

(1) If

$$n^2+n+1 = m_1m_2,$$

we can choose A, B, C and D such that

(2)

$$m_1 = A^2+C^2+AC,$$

$$m_2 = B^2+D^2+BD, \tag{3}$$

and

$$AD-BC = \pm 1. \tag{4}$$

It is well known that all factors of n^2+n+1 are of the form k^2+l^2+kl. Therefore we have only to prove that A B, C and D can be chosen to satisfy (4).

LEMMA 1.—If m_1 is prime, the theorem is true.

Let
$$m_1 = A^2+C^2+AC.$$

As
$$n^2+n+1 = m_1 m_2.$$

$$m_2 = \frac{n^2+n+1}{m_1} = \frac{(n^2+n+1)(A^2+C^2+AC)}{m_1^2}$$

$$= \left(\frac{An-C}{m_1}\right)^2 + \left[\frac{C(n+1)+A}{m_1}\right]^2 + \left(\frac{An-C}{m_1}\right)\left[\frac{C(n+1)+A}{m_1}\right].$$

Now

$$\begin{aligned}(An-C)(Cn-A) &= ACn^2-n(A^2+C^2)+AC \\ &\equiv \{ACn^2-n(A^2+C^2-A^2-C^2-AC)+AC\} \pmod{m_1} \\ &\equiv AC(n^2+n+1) \pmod{m_1} \\ &\equiv 0 \pmod{m_1}\end{aligned}$$

m_1 being a prime, one at least of $(An-C)$ and $(Cn-A)$ is a multiple of m_1.

In case it is only the latter, replace C by A and A by C so that in all cases we have

$$m_1 = A^2+C^2+AC$$

and

$$An-C \equiv 0 \pmod{m_1}. \tag{5}$$

Now

$$\begin{aligned}0 &\equiv n(An-C) \pmod{m_1} \\ &\equiv An^2-Cn \pmod{m_1} \\ &\equiv -Cn+A(n^2-n^2-n-1) \pmod{m_1} \\ &\equiv -Cn-A-An \pmod{m_1} \\ &\equiv -Cn-A-C \pmod{m_1} \\ &\text{[because of (5)].}\end{aligned}$$

Therefore

$$m_2 = B^2+D^2+BD$$

where B and D are integers given by

$$B = \frac{An-C}{m_1} \quad \text{and} \quad D = \frac{C(n+1)+A}{m_1}.$$

Now

$$\begin{aligned}AD-BC &= \frac{ACn+AC+A^2-ACn+C^2}{m_1} \\ &= 1.\end{aligned}$$

Therefore the lemma is true.

LEMMA 2.—If

$$n^2+n+1 = m_1m_2$$

and

(i) $m_1 = mp_2$, p_2 being a prime number

(ii) $m = a^2+c^2+ac$

(iii) $p_2m_2 = b^2+d^2+bd$

(iv) $ad-bc = 1$,

then we can choose A, B, C and D such that

$$m_1 = A^2+C^2+AC$$
$$m_2 = B^2+D^2+BD$$

and

$$AD-BC = \pm 1.$$

p_2, being a factor of n^2+n+1, is equal to e^2+f^2+ef where e and f are suitable integers.

As

$$p_2m_2 = b^2+d^2+bd,$$

$$m_2 = \frac{b^2+d^2+bd}{e^2+f^2+ef} = \frac{(b^2+d^2+bd)(e^2+f^2+ef)}{{p_2}^2}$$

$$= \left(\frac{be-df}{p_2}\right)^2+\left(\frac{bf+de+df}{p_2}\right)^2+\left(\frac{be-df}{p_2}\right)\left(\frac{bf+de+df}{p_2}\right).$$

Now

$$\begin{aligned}(be-df)(de-bf) &= bde^2+bdf^2-efb^2-efd^2\\ &\equiv [bd(e^2+f^2-e^2-f^2-ef)-ef(b^2+d^2)] \pmod{p_2}\\ &\equiv -ef(b^2+d^2+bd) \pmod{p_2}\\ &\equiv 0 \pmod{p_2}\end{aligned}$$

p_2 being a prime, one at least of $(be-df)$ and $(de-bf)$ is a multiple of p_2. In case it is not the former, replace e and f by $-f$ and $-e$ respectively so that in all cases we have

$$p_2 = e^2+f^2+ef$$

and

$$be-df \equiv 0 \pmod{p_2}.$$

Now

$$\begin{aligned}0 &\equiv be-df \pmod{p_2}\\ &\equiv b^2e-bdf \pmod{p_2}\\ &\equiv e(b^2-b^2-d^2-bd)-bdf \pmod{p_2}\\ &\equiv -d(ed+be+bf) \pmod{p_2}\\ &\equiv -d(ed+df+bf) \pmod{p_2}.\end{aligned}$$

Therefore $ed+df+bf$ is a multiple of p_2 for, if not, d must be a multiple of p_2 and hence on account of (iii) lemma 2, b and therefore $ed+df+bf$ is a multiple of p_2.

Now we have

$$m_2 = B^2+D^2+BD$$

where B and D are integers given by

$$B = \frac{be-df}{p_2}, \quad D = \frac{bf+df+de}{p_2}.$$

Also

$$\begin{aligned} m_1 = mp_2 &= (a^2+c^2+ac)(e^2+f^2+ef) \\ &= (ae-cf)^2+(af+ce+cf)^2+(ae-cf)(af+ce+cf) \\ &= A^2+C^2+AC \end{aligned}$$

where

$$A = ae-cf \quad \text{and} \quad C = af+ce+cf$$

$$\begin{aligned} AD-BC &= \frac{(ae-cf)(bf+df+de)-(be-cf)(af+cf+ce)}{p_2} \\ &= ad-bc = 1, \end{aligned}$$

the lemma is true.

The main theorem of this section (with $AD-BC = 1$) can now be proved by combining the two lemmas and using the method of induction.

To prove that the theorem is true with $AD-BC = -1$ also we have only to replace A and C by $-A$ and $-C$ respectively.

Reference.

Vaidyanathaswamy, R. (1928). On integer roots of the unit matrix. *Jour., Lond. Math. Soc.*, 3.