2. C. C. MacDuffee, *The theory of matrices*, Ergebnisse der Mathematik und ihrer Grenzgebiete, New York, Chelsea, 1946, pp. 31–36.

3. J. H. Bell, *Left associates of monic matrices, with an application to unilateral matrix equations*, Amer. J. Math. vol. 71 (1949).

4. W. E. Roth, *On the unilateral equation in matrices*, Trans. Amer. Math. Soc. vol. 32 (1930) p. 67.

5. J. H. Bell, *Families of solutions of the unilateral matrix equation*, Proceedings of the American Mathematical Society vol. 1 (1950) pp. 152, 157.

6. ———, *The solution of a unilateral direct product matrix equation*, Proceedings of the American Mathematical Society vol. 1 (1950) pp. 777–781.

MICHIGAN STATE COLLEGE

ON MAGIC SQUARES CONSTRUCTED BY THE UNIFORM STEP METHOD

T. M. APOSTOL AND HERBERT S. ZUCKERMAN

An application of the theory of congruences to the study of magic squares constructed by the uniform step method was first given by D. N. Lehmer.[1] The n^2 cells of the square are denoted by two coordinates (A, B), A being the number of the column counting from the left and B the number of the row counting from the bottom. Lehmer summed up the uniform step process in the following congruences for determining the cell (A_x, B_x) into which the number x is entered:

$$A_x \equiv p + \alpha(x-1) + a\left[\frac{x-1}{n}\right] \pmod{n}, \tag{1}$$

$$B_x \equiv q + \beta(x-1) + b\left[\frac{x-1}{n}\right] \pmod{n}, \tag{2}$$

where (p, q) is the cell into which the number 1 is entered, (α, β) is the "step" used in proceeding from one cell to another, (a, b) is the "break-step" that must be used when an occupied cell is arrived at, and the symbol $[k]$ denotes the greatest integer contained in k. Lehmer proved the following theorems:

Presented to the Society, November 25, 1950; received by the editors August 21, 1950.

[1] D. N. Lehmer, *On the congruences connected with certain magic squares*, Trans. Amer. Math. Soc. vol. 31 (1929) pp. 529–551. Definitions of the terms "magic," "diabolic," and "symmetric" are given in this paper.

THEOREM A. *A necessary and sufficient condition that congruences* (1) *and* (2) *fill the square is that the determinant*

$$\begin{vmatrix} \alpha & a \\ \beta & b \end{vmatrix}$$

shall be prime to n.

If the condition of Theorem A holds, we have further the following theorem:

THEOREM B. *The square will be magic if and only if the numbers* α, β, a, *and* b *are all prime to* n.

The magic squares obtained by this method have the property that the numbers in any column or those in any row form a complete system of incongruent numbers modulo n and no two numbers in the system lie between the same two multiples of n. Squares with this property will be referred to here as *regular squares*. It is elementary to show that all regular squares are magic, although of course, there are magic squares that are not regular.

In this paper we extend the study of the uniform step method by considering the more general situation where the numbers α, β, a, b, and

$$\begin{vmatrix} \alpha & a \\ \beta & b \end{vmatrix}$$

are not all prime to n. We shall not consider the problem in its fullest generality but shall restrict ourselves to the cases where

$$\begin{aligned} (\alpha, n) &= (\beta, n) = \delta, \\ (a, n) &= (b, n) = \epsilon, \\ (\delta, \epsilon) &= 1, \\ (\alpha b - a\beta, n) &= \delta\epsilon\theta. \end{aligned}$$

These conditions are not as restrictive as may appear at first sight. For example, it can be shown that (α, n) must be the same as (β, n) and that (δ, ϵ) must be 1 if we are to obtain regular squares by our alteration of the method. The special case considered by Lehmer is obtained when $\delta = \epsilon = \theta = 1$.

To construct the square we insert the number 1 in the cell (p, q) chosen arbitrarily. The number 2 is entered in the cell $(p+\alpha, q+\beta)$, 3 in cell $(p+2\alpha, q+2\beta)$, and so on, the coordinates always being reduced modulo n. When the step (α, β) is used n/δ times it places the

number $n/\delta+1$ in the cell $(p+\alpha n/\delta, q+\beta n/\delta)$. Since δ divides α and β, this cell is the same, modulo n, as the initial cell (p, q). Thus the step (α, β) is seen to fail after n/δ uses. Furthermore, this is the first such duplication, for the congruence $\lambda\alpha \equiv \mu\alpha \pmod{n}$ implies $\lambda-\mu \equiv 0 \pmod{n/\delta}$ since $(\alpha, n)=\delta$, and therefore the step (α, β) could not have failed until the number $n/\delta+1$ was arrived at. At this point the break-step (a, b) is used to place $n/\delta+1$ in the cell $(p+a, q+b)$. The step (α, β) is again resorted to and $n/\delta+2$ is inserted in $(p+a+\alpha, q+b+\beta)$, $n/\delta+2$ in $(p+a+2\alpha, q+b+2\beta)$, and so on. The number $2n/\delta+1$ would fall in $(p+a+\alpha n/\delta, q+b+\beta n/\delta) \equiv (p+a, q+b) \pmod{n}$, and the break-step (a, b) is used for the second time, provided, of course, that no other duplications have occurred since inserting $n/\delta+1$. For the moment we shall not be concerned with any duplications which may occur between multiples of n/δ and we agree to use the break-step (a, b) only after every n/δ numbers are inserted, even if this necessitates placing two numbers in the same cell. As long as this procedure is adhered to, the coordinates (A_x, B_x) of the cell into which the number x is entered will be given by the congruences:

$$A_x \equiv p + \alpha(x-1) + a\left[\frac{(x-1)\delta}{n}\right] \pmod{n}, \tag{3}$$

$$B_x \equiv q + \beta(x-1) + b\left[\frac{(x-1)\delta}{n}\right] \pmod{n}. \tag{4}$$

These formulas will be used until the number $x_1 = n^2/(\delta\epsilon\theta)+1$ is arrived at, that is, until the break-step (a, b) has been used $n/(\theta\epsilon)$ times. At this point the break-step (a, b) fails. In fact, the numbers

$$x_k = kn^2/(\delta\epsilon\theta) + 1 \quad (k = 1, 2, \cdots, \delta\epsilon\theta - 1)$$

will be placed in the cells given by $(p+kan/(\theta\epsilon), q+kbn/(\theta\epsilon))$, and these cells will be already occupied by the numbers $x_k' = 1 + h_k$, where each h_k is defined as that solution of the congruence

$$h_k\alpha/\delta \equiv kan/(\delta\epsilon\theta) \pmod{n/\delta} \tag{5}$$

which lies in the range $0 \leqq h_k < n/\delta$. Each of these can always be solved since $(\alpha, n)=\delta$ and each will yield an h_k in the desired range so that we shall have

$$x_k' < x_k \quad \text{and} \quad \left[\frac{(x_k'-1)\delta}{n}\right] = 0,$$

for all k considered. To find the cells into which the x_k' fall, we have,

from (5), $\alpha\beta h_k \equiv (ka\beta n/(\theta\epsilon)) \pmod{\delta n}$. Since $(\alpha b - a\beta,\ n) = \delta\epsilon\theta$, we may write $a\beta = b\alpha + t\delta\epsilon\theta$ in the right member of this last congruence to obtain $\alpha\beta h_k \equiv (knb\alpha/(\theta\epsilon)) \pmod{\delta n}$, $\beta h_k \equiv (knb/(\theta\epsilon)) \pmod{n}$. By (5) we also have $\alpha h_k \equiv (kna/(\theta\epsilon)) \pmod{n}$ so that (3) and (4) now yield

$$A'_{xk} \equiv p + \alpha h_k \equiv p + kan/(\theta\epsilon) \pmod{n},$$

$$B'_{xk} \equiv q + \beta h_k \equiv q + kbn/(\theta\epsilon) \pmod{n}.$$

Hence each x'_k already occupies the cell into which x_k will be placed.

We now introduce a *second* break-step (c, d) which is used after every $n^2/(\delta\epsilon\theta)$ numbers are inserted to avoid the duplications that occur at these points. The formulas for locating the cell (A_x, B_x) into which x falls now become:

$$(6)\quad A_x \equiv p + \alpha(x-1) + a\left[\frac{(x-1)\delta}{n}\right] + c\left[\frac{(x-1)\delta\epsilon\theta}{n^2}\right] \pmod{n},$$

$$(7)\quad B_x \equiv q + \beta(x-1) + b\left[\frac{(x-1)\delta}{n}\right] + d\left[\frac{(x-1)\delta\epsilon\theta}{n^2}\right] \pmod{n}.$$

The square formed by these congruences clearly depends on the numbers $\alpha, \beta, a, b, c, d$, and may be denoted by the matrix

$$\begin{pmatrix} \alpha & a & c \\ \beta & b & d \end{pmatrix}.$$

The process may or may not fill the square, and when it does, the resulting square may or may not be magic. In this connection we shall proved the following theorems:[2]

THEOREM 1. *The square constructed according to congruences* (6) *and* (7) *will be filled if and only if we have*

$$(bc - ad,\ \delta\epsilon\theta) = \epsilon$$

and

$$(\beta c - \alpha d,\ \delta\epsilon\theta) = \delta.$$

THEOREM 2. *If* $\theta = 1$, *the resulting square will be regular (and hence magic) if and only if c and d are both prime to* $\delta\epsilon$.

PROOF OF THEOREM 1. We begin by writing each number x_i in the form

$$(8)\qquad x_i = 1 + \rho_i n^2/(\delta\epsilon\theta) + \sigma_i n/\delta + \tau_i,$$

[2] We note that the conditions of Theorems 1 and 2 require n to be odd.

where

$$0 \leqq \tau_i \leqq n/\delta - 1, \quad 0 \leqq \sigma_i \leqq n/(\theta\epsilon) - 1, \quad 0 \leqq \rho_i \leqq \delta\epsilon\theta - 1.$$

We then have

$$(9) \qquad \left[\frac{(x_i - 1)\delta\epsilon\theta}{n^2}\right] = \rho_i \quad \text{and} \quad \left[\frac{(x_i - 1)\delta}{n}\right] = \rho_i n/(\theta\epsilon) + \sigma_i,$$

since we have

$$0 \leqq \left[\frac{(x_i - 1)\delta\epsilon\theta}{n^2}\right] - \rho_i = [\sigma_i\theta\epsilon/n + \tau_i\delta\epsilon\theta/n^2]$$

$$\leqq \sigma_i\theta\epsilon/n + \tau_i\delta\epsilon\theta/n^2 \leqq 1 - \theta\epsilon/n + \theta\epsilon/n - \delta\epsilon\theta/n^2 < 1,$$

and

$$0 \leqq \left[\frac{(x_i - 1)\delta}{n}\right] - (\rho_i n/(\theta\epsilon) + \sigma_i) = [\tau_i\delta/n] = 0.$$

Formulas (6) and (7) become, upon simplifying,

$$A_{x_i} \equiv p + \alpha\tau_i + a(\rho_i n/(\theta\epsilon) + \sigma_i) + c\rho_i \pmod{n},$$

$$B_{x_i} \equiv q + \beta\tau_i + b(\rho_i n/(\theta\epsilon) + \sigma_i) + d\rho_i \pmod{n},$$

where we have used (9) and the definitions of δ, ϵ, θ.

If $x_2 > x_1$ are two numbers in the same cell, then we have

$$(10) \quad (an/(\theta\epsilon) + c)(\rho_1 - \rho_2) + a(\sigma_1 - \sigma_2) + \alpha(\tau_1 - \tau_2) \equiv 0 \pmod{n},$$

$$(11) \quad (bn/(\theta\epsilon) + d)(\rho_1 - \rho_2) + b(\sigma_1 - \sigma_2) + \beta(\tau_1 - \tau_2) \equiv 0 \pmod{n},$$

from which we obtain

$$(12) \qquad \begin{aligned} (bc - ad)(\rho_1 - \rho_2) + (\alpha b - \beta a)(\tau_1 - \tau_2) &\equiv 0 \pmod{n}, \\ (\beta c - \alpha d)(\rho_1 - \rho_2) + (\beta a - \alpha b)(\sigma_1 - \sigma_2) &\equiv 0 \pmod{n}. \end{aligned}$$

Therefore we have

$$(bc - ad)(\rho_1 - \rho_2) \equiv 0 \pmod{\delta\epsilon\theta} \text{ and } (\beta c - \alpha d)(\rho_1 - \rho_2) \equiv 0 \pmod{\delta\epsilon\theta}.$$

Using the hypothesis of the theorem we may write

$$\rho_1 - \rho_2 \equiv 0 \pmod{\delta\theta} \quad \text{and} \quad \rho_1 - \rho_2 \equiv 0 \pmod{\epsilon\theta}.$$

Since $(\delta, \epsilon) = 1$, these congruences imply $\rho_1 - \rho_2 \equiv 0 \pmod{\delta\epsilon\theta}$ which, in virtue of the inequality $0 \leqq \rho_i < \delta\epsilon\theta$, implies $\rho_1 = \rho_2$.

From congruences (12) we now obtain, since $(\alpha b - a\beta, n) = \delta\epsilon\theta$,

$$\tau_1 - \tau_2 \equiv 0 \pmod{n/(\delta\epsilon\theta)}, \qquad \sigma_1 - \sigma_2 \equiv 0 \pmod{n/(\delta\epsilon\theta)}.$$

If we write $\tau_1-\tau_2=\tau n/(\delta\epsilon\theta)$ and $\sigma_1-\sigma_2=\sigma n/(\delta\epsilon\theta)$, where $0\leqq|\tau|\leqq\theta\epsilon-1$, $0\leqq|\sigma|\leqq\delta-1$, congruences (10), (11) become

$$a n\sigma/(\delta\epsilon\theta)+\alpha n\tau/(\delta\epsilon\theta)\equiv 0 \pmod{n},$$
$$b n\sigma/(\delta\epsilon\theta)+\beta n\tau/(\delta\epsilon\theta)\equiv 0 \pmod{n},$$

from which we obtain

$$\begin{aligned} a\sigma+\alpha\tau &\equiv 0 \pmod{\delta\epsilon\theta},\\ b\sigma+\beta\tau &\equiv 0 \pmod{\delta\epsilon\theta}. \end{aligned} \tag{13}$$

Hence $a\sigma\equiv 0 \pmod{\delta}$, but $(a,\delta)=(\epsilon,\delta)=1$, so that $\sigma\equiv 0 \pmod{\delta}$, but $0\leqq|\sigma|<\delta$ and hence $\sigma=0$.

Formulas (13) now gives us $\alpha\tau\equiv 0 \pmod{\delta\epsilon\theta}$, $\beta\tau\equiv 0 \pmod{\delta\epsilon\theta}$, so that

$$(\alpha d-\beta c)\tau\equiv 0 \pmod{\delta\epsilon\theta},$$

and using the hypothesis we have $\tau\equiv 0 \pmod{\theta\epsilon}$, but $0\leqq|\tau|<\theta\epsilon$ so that $\tau=0$ and $x_1=x_2$. Thus if the conditions of Theorem 1 are fulfilled, two different numbers cannot fall in the same cell and hence the square will be filled since there are exactly n^2 numbers and n^2 cells.

The conditions of Theorem 1 are also necessary, for if the process fills the square, we can find an x to satisfy (6) and (7) for every pair of integers (A_x, B_x). This means that given any pair of integers r, s, we can always find x, z, w to satisfy

$$\alpha x+az+cw\equiv r, \qquad \beta x+bz+dw\equiv s \pmod{n},$$

where we have written

$$r=A_x-p+\alpha, \qquad s=B_x-q+\beta,$$
$$z=\left[\frac{(x-1)\delta}{n}\right], \qquad w=\left[\frac{(x-1)\delta\epsilon\theta}{n^2}\right].$$

From the last two congruences we have

$$(\alpha b-a\beta)x+(bc-ad)w\equiv br-as \pmod{n}$$

and

$$(\alpha b-a\beta)z+(\alpha d-\beta c)w\equiv \alpha s-\beta r \pmod{n}.$$

Using the definition of θ these give us

$$(\beta c-\alpha d)w\equiv \beta r-\alpha s \pmod{\delta\epsilon\theta}$$

and

$$(bc - ad)w \equiv br - as \pmod{\delta\epsilon\theta}.$$

Suppose now $(bc-ad,\ \delta\epsilon\theta)=\epsilon\gamma$ and $(\beta c-\alpha d,\ \delta\epsilon\theta)=\delta\zeta$. Then taking $r=0$, $s=1$ in the last congruence we find $\epsilon\gamma \mid a$. But $\epsilon\gamma \mid \delta\epsilon\theta$ and $\delta\epsilon\theta \mid n$. Hence $\epsilon\gamma \mid (a,\ n)=\epsilon$, so that $\gamma=1$. Similarly we can show that $\zeta=1$ and the proof of Theorem 1 is complete.

Summing up, we can describe the construction of the square as follows: The number 1 is entered into the cell $(p,\ q)$. Each further x is entered by making the step $(\alpha,\ \beta)$ from the cell occupied by $x-1$. Whenever the cell arrived at is already filled, the first break-step $(a,\ b)$ is also made. If the first break-step $(a,\ b)$ still leads to an occupied cell, then the second break-step $(c,\ d)$ is used. The conditions of Theorem 1 are necessary and sufficient for success in filling the square by this method.

PROOF OF THEOREM 2. If two numbers $x_1>x_2$ are in the same column, then congruence (10) holds. The numbers x_1 and x_2 cannot lie between the same two multiples of n, for if we have $[(x_1-1)/n] = [(x_2-1)/n]$, using (8) we may write

$$\rho_1 n/(\delta\epsilon\theta) + [\sigma_1/\delta + \tau_1/n] = \rho_2 n/(\delta\epsilon\theta) + [\sigma_2/\delta + \tau_2/n], \tag{14}$$

from which we have

$$0 \leqq \rho_1 - \rho_2 = \frac{\delta\epsilon\theta}{n}\left([\sigma_2/\delta + \tau_2/n] - [\sigma_1/\delta + \tau_1/n]\right)$$

$$\leqq \frac{\delta\epsilon\theta}{n}\left(\frac{n}{\delta\epsilon\theta} - \frac{1}{\delta} + \frac{1}{\delta} - \frac{1}{n}\right) < \frac{\delta\epsilon\theta}{n}\,\frac{n}{\delta\epsilon\theta} = 1,$$

where we have used $0\leqq\sigma_i\leqq n/(\theta\epsilon)-1$, $0\leqq\tau_i\leqq n/\delta-1$. Since the ρ_i are integers, this implies $\rho_1=\rho_2$. Congruence (10) now becomes $a(\sigma_1-\sigma_2)+\alpha(\tau_1-\tau_2)\equiv 0 \pmod{n}$, and since $(a,\ \delta)=1$ and $\delta \mid \alpha$ we have

$$\sigma_1 - \sigma_2 \equiv 0 \pmod{\delta}. \tag{15}$$

But by (14) we have $[\sigma_1/\delta+\tau_1/n]=[\sigma_2/\delta+\tau_2/n]=s$, say, from which we may write

$$s\delta \leqq \sigma_2 + \tau_2\delta/n \leqq \sigma_1 + \tau_1\delta/n \leqq s\delta + \delta - 1/n. \tag{16}$$

Since $0\leqq\tau_2\delta/n<1$ and σ_2 is an integer, the first inequality in (16) implies $\sigma_2\geqq s\delta$. Subtracting this from the last inequality in (16) we obtain

$$0 \leqq \sigma_1 - \sigma_2 \leqq s\delta + \delta - 1/n - s\delta = \delta - 1/n < \delta.$$

Since the σ_i are integers, this last relation, with (15), implies $\sigma_1=\sigma_2$, and congruence (10) now gives us $\alpha(\tau_1-\tau_2)\equiv 0 \pmod{n}$, $\tau_1-\tau_2$

$\equiv 0 \pmod{n/\delta}$, but we have $0 \leqq \tau_i < n/\delta$ so that $\tau_1 = \tau_2$ and hence $x_1 = x_2$. Thus the method will not enter into the same column two numbers which lie between the same two multiples of n and a similar argument proves this for the rows as well. (Note that we have not yet used any of the hypotheses of Theorem 2.)

It remains to show that two congruent numbers will not fall in the same row or column. The problem of obtaining necessary and sufficient conditions to ensure this for general θ is open and appears to be quite difficult. The case $\theta = 1$ is governed by the conditions of Theorem 2 and we complete the proof in this case. If we have $x_1 \equiv x_2 \pmod{n}$, then we may write

$$x_1 - x_2 = (\rho_1 - \rho_2)n^2/(\delta\epsilon) + (\sigma_1 - \sigma_2)n/\delta + \tau_1 - \tau_2 \equiv 0 \pmod{n},$$

from which we have $\tau_1 - \tau_2 \equiv 0 \pmod{n/\delta}$ and hence $\tau_1 = \tau_2$. Consequently we have $(\sigma_1 - \sigma_2)n/\delta \equiv 0 \pmod{n}$, $\sigma_1 - \sigma_2 \equiv 0 \pmod{\delta}$. We now write $\sigma_1 - \sigma_2 = \sigma\delta$, where $0 \leqq |\sigma| \leqq n/(\delta\epsilon) - 1$. If x_1 and x_2 are in the same column, then congruence (10) holds and now becomes

$$c(\rho_1 - \rho_2) + a\sigma\delta \equiv 0 \pmod{n}. \tag{17}$$

Since $\epsilon | a$ we obtain $c(\rho_1 - \rho_2) \equiv 0 \pmod{\delta\epsilon}$ and the hypothesis $(c, \delta\epsilon) = 1$ implies $\rho_1 - \rho_2 \equiv 0 \pmod{\delta\epsilon}$, which, with the inequality $0 \leqq \rho_i < \delta\epsilon$, yields $\rho_1 = \rho_2$. Then by (17) we have $\sigma \equiv 0 \pmod{n/(\delta\epsilon)}$ and since $0 \leqq |\sigma| < n/(\delta\epsilon)$, we have $\sigma = 0$, $x_1 = x_2$. A similar argument for the rows proves that the conditions of Theorem 2 are sufficient.

The conditions are also necessary, for if $(c, \delta\epsilon) = \eta > 1$ we can show that the two congruent numbers $x_1 = 1$ and $x_2 = 1 + n^2/\eta + tn$ fall in the same column, where t is defined as that solution of the congruence $ta/\epsilon \equiv -c/\eta \pmod{n/(\delta\epsilon)}$ which satisfies the inequality $0 \leqq t < n/(\delta\epsilon)$. Since $(a/\epsilon, n/(\delta\epsilon)) = 1$, such a t exists. By hypothesis, $\eta \geqq 2$. (We may also assume $\delta\epsilon \geqq 2$, since $\delta\epsilon = 1$ is Lehmer's case.) We then have

$$\begin{aligned} x_2 = 1 + n^2/\eta + tn &\leqq 1 + n^2/\eta + n^2/(\delta\epsilon) - n \\ &\leqq 1 + n^2/2 + n^2/2 - n = n^2 - (n-1) < n^2, \end{aligned}$$

which shows that x_2 is a permissible value. Furthermore, we have

$$\begin{aligned} A_{x_2} &\equiv p + \alpha(n^2/\eta + tn) + a[n\delta/\eta + t\delta] + c[\delta\epsilon/\eta + t\delta\epsilon/n] \\ &\equiv p + at\delta + c\delta\epsilon/\eta \pmod{n}, \end{aligned}$$

since $\eta | a\delta$ and $[t\delta\epsilon/n] = 0$. The definition of t shows that $A_{x_2} \equiv p \pmod{n}$ so that x_1 and x_2 lie in the same column. Hence if $(c, \delta\epsilon) > 1$ the square will not be regular. A similar argument shows that the

condition $(d, \delta\epsilon) = 1$ is also necessary and the proof of Theorem 2 is complete.

Lehmer's analysis for determining whether or not a square obtained by the uniform step method is diabolic or symmetric can be applied here to yield the following theorems, the proofs of which we omit since they parallel those in Lehmer's paper.

THEOREM 3. *When* $\theta = 1$, *the magic square constructed by means of congruences* (6) *and* (7) *will be diabolic if and only if*

$$(c + d, \delta\epsilon) = (c - d, \delta\epsilon) = 1.$$

THEOREM 4. *The square constructed by means of* (6) *and* (7) *will be symmetric if and only if*

$$2p \equiv 1 + \alpha + a - c(\delta\epsilon\theta - 1) \pmod{n},$$
$$2q \equiv 1 + \beta + b - d(\delta\epsilon\theta - 1) \pmod{n}.$$

The square, of course, can be symmetric without being magic. We observe that when n is a multiple of 3, Theorem 3 cannot be satisfied so that, as in Lehmer's case, our method will not yield diabolic squares for such n. However, our method can yield magic squares which are also magic along the main diagonal (extending from the upper left to the lower right corners of the square) and along those parallel to it, when $n \equiv 0 \pmod 3$. For example, when $n = 9$, the square given by

$$\begin{pmatrix} \alpha & a & c \\ \beta & b & d \end{pmatrix} = \begin{pmatrix} 3 & 1 & 1 \\ 3 & 2 & 1 \end{pmatrix}$$

has this property. This kind of square cannot occur in Lehmer's case since his conditions require all seven numbers α, β, a, b, $\alpha+\beta$, $a+b$, $\alpha b - a\beta$ to be prime to 3 and this is impossible.

CALIFORNIA INSTITUTE OF TECHNOLOGY AND
UNIVERSITY OF WASHINGTON