ELSEVIER Linear Algebra and its Applications 318 (2000) 195–208

LINEAR ALGEBRA AND ITS APPLICATIONS

www.elsevier.com/locate/laa

Systems of linear congruences with individual moduli

David C. Torney [a,*], Jun Wang [b]

[a] T-10, MS K710, Los Alamos National Laboratory, Los Alamos, NM 87545, USA
[b] Department of Applied Mathematics, Institute of Mathematical Sciences, Dalian University of Technology, Dalian 116024, People's Republic of China

Received 3 November 1998; accepted 16 May 2000

Submitted by H. Schneider

Abstract

Consider an $n \times n$ matrix A, with integer elements, a column vector x of n integer indeterminates, and a column vector Q of n integers greater than unity. Ax modulo Q constitutes another n-vector b of nonnegative integers. The elemental feature of interest for such systems is whether they are regular (i.e., nonsingular): whether b uniquely determines x modulo Q. Let P_σ denote the permutation matrix corresponding to a permutation σ of $\{1, 2, \ldots, n\}$. Then, for the special case of all pairs of elements of Q having the same greatest common factor, it is established that regularity obtains if and only if there exists a permutation σ so that $P_\sigma A P_\sigma^{\mathrm{T}}$ is a triangular matrix with each element on the main diagonal coprime to its respective modulus (from $P_\sigma Q$). To resolve systems with general Q, a set of moduli is first derived from each original modulus by factoring it into prime-power factors. We introduce a corresponding regularity-preserving transformation of A and Q into an A' and Q': the latter containing, exclusively, prime-power moduli. Elementary transformations of A' preserving regularity modulo Q'—denoted equivalences—are introduced. A' is shown to be regular modulo Q' if and only if there exists a permutation σ so that $P_\sigma A' P_\sigma^{\mathrm{T}}$ is equivalent to a triangular matrix, having each element on the main diagonal coprime to its respective modulus (from $P_\sigma Q'$). Whence, regularity is fully resolved for general systems. An algorithm for solving an arbitrary regular system $Ax \equiv b \pmod{Q}$ is, furthermore, implicit in these results. © 2000 Elsevier Science Inc. All rights reserved.

AMS classification: Primary 11D79; Secondary 11A07; 14D99; 15A36

Keywords: Systems of linear congruences; Nonassociative algebra

* Corresponding author.
E-mail addresses: dct@lanl.gov (D.C. Torney), junwang@dlut.edu.cn (J. Wang).

PII: S 0 0 2 4 - 3 7 9 5 (0 0) 0 0 1 7 3 - 7

1. Introduction

Let $Q = (q_1, q_2, \ldots, q_n)^{\mathrm{T}}$ be a vector of natural numbers, each larger than unity (but otherwise unrestricted), and let $\mathscr{V} = \mathscr{V}(Q) = \{v = (v_1, \ldots, v_n)^{\mathrm{T}}\colon\ 0 \leqslant v_i < q_i,\ i = 1, 2, \ldots, n\}$. For any integer vector $w = (w_1, \ldots, w_n)^{\mathrm{T}}$, there is clearly a unique $v \in \mathscr{V}$ of representatives satisfying

$$w_i \equiv v_i \pmod{q_i}, \quad i = 1, 2, \ldots, n.$$

In this case we write $w \equiv v \pmod{Q}$.

Definition 1.1. Let A be in $M_n(\mathbb{Z})$, the set of $n \times n$ matrices with integer elements. Then A is called *Q-regular* (or, simply, *regular*) if the map

$$\phi_{A;Q} : v \longrightarrow Av \pmod{Q}, \quad v \in \mathscr{V}(Q),$$

is a permutation on $\mathscr{V}$, where Av denotes conventional matrix multiplication and where (mod Q) has the given meaning.

The question addressed herein is: What are the characteristics of Q-regular matrices in $M_n(\mathbb{Z})$? From its definition, we see that when all of the entries of Q are equal, Q-regularity of A obtains if and only if A is an invertible matrix over the ring of residues modulo q, i.e., $(\det\ A, q) = 1$ (cf. [7, Theorem 2.1, p. 96])—a central theorem in the classical theory of linear systems over commutative rings [2].

In greater detail, when all entries of Q are equal, any matrix in $M_n(\mathbb{Z})$ is convertible into a diagonal matrix in Smith normal form by three types of elementary transformations [5, vol. 5, pp. 471, 472; vol. 6, p. 470]. In fact, these transformations constitute the basis of the theory of systems of linear equations over commutative rings. On the other hand, when Q contains two, or more, distinct integers, these transformations do not, in general, preserve regularity, signalling the novelty of the question at hand.

The idiosyncrasy of systems of linear congruences modulo Q is amply illustrated by the consideration of successive mappings: $\phi_{A;Q}$ followed by $\phi_{B;Q}$. In general, the composite mapping does not equal $\phi_{C;Q}$, with $C \equiv BA \pmod{Q}$, because matrix multiplication modulo Q is plainly nonassociative.

In Section 3, regularity is resolved for the special case with greatest common divisor $(q_i, q_j) = r,\ 1 \leqslant i < j \leqslant n$. For this case, a Q-regular matrix is shown to be, essentially, triangular. In Section 4, Q-regularity-preserving transformations, denoted equivalences, are described. Also, in this section, a regularity-preserving transformation of systems into new systems in which the elements of the new Q's are powers of primes (which are not necessarily distinct) is described. In Section 5, regular matrices are characterized for such Q's: Theorem 5.1 establishes that a Q-regular matrix is equivalent to a triangular matrix under the transformations introduced in Section 4.

These results constitute a primary generalization of linear algebra in the ring of residues modulo q, suggesting a host of analogous theorems in various ring-theoretic settings. The triangular system derived from a regular system is easily solved, and reversing the processes used to generate it will solve the original system.

Every new mathematical result engenders applications. Here, for instance, we may now implement linear rearrangements of the integer points within finite orthotopes, q_i being the edge length, $i = 1, 2, \ldots, n$. (An orthotope is the $\mathbb{R}^n$-analogue of a rectangle in $\mathbb{R}^2$, viz., [3, p. 123].)

2. Preliminary lemmas

We first give, as lemmas, two simple but useful criteria of regularity.

Lemma 2.1. *Let A be in $M_n(\mathbb{Z})$ and let $Q = (q_1, q_2, \ldots, q_n)^{\mathrm{T}}$. Then A is Q-regular if and only if there is no $v = (v_1, \ldots, v_n)^{\mathrm{T}} \neq 0$ with $|v_i| < q_i$ such that $Av \equiv 0$ (mod Q).*

Proof. Since $\mathscr{V}$ is finite, $\phi_{A;Q}$ is bijective if and only if it is injective. Therefore, A is Q-regular if and only if for any $v, v' \in \mathscr{V}$ with $v \neq v'$, $Av \not\equiv Av'$ (mod Q), or equivalently, $A(v - v') \not\equiv 0 = (0, \ldots, 0)^{\mathrm{T}}$ (mod Q). □

For example, if

$$A\begin{pmatrix} 1 \\ -1 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{Q},$$

then

$$A\begin{pmatrix} 1 \\ 0 \end{pmatrix} \equiv A\begin{pmatrix} 0 \\ 1 \end{pmatrix} \pmod{Q},$$

and $\phi_{A;Q}$ is not injective.

Lemma 2.2. *Let A be in $M_n(\mathbb{Z})$, let $Q = (q_1, q_2, \ldots, q_n)^{\mathrm{T}}$, and let $rQ = (rq_1, rq_2, \ldots, rq_n)^{\mathrm{T}}$, where r is any positive integer. Then A is rQ-regular if and only if A is Q-regular and $(r, \det A) = 1$.*

To construct a proof, consider the following three congruence systems:

$$Ax \equiv 0 \pmod{rQ}, \tag{2.1}$$

$$Ay \equiv 0 \pmod{Q}, \tag{2.2}$$

and

$$Az \equiv 0 \pmod{r}, \tag{2.3}$$

where $x = (x_1, x_2, \ldots, x_n)^{\mathrm{T}}$, $y = (y_1, y_2, \ldots, y_n)^{\mathrm{T}}$, and $z = (z_1, z_2, \ldots, z_n)^{\mathrm{T}}$.

Proof of Lemma 2.2. *Sufficiency*: Suppose that A is Q-regular and $(\det A, r) = 1$. In this case, if there is a solution of (2.1) $u = (u_1, u_2, \ldots, u_n)^{\mathrm{T}}$, with $|u_i| < rq_i$, $i = 1, 2, \ldots, n$, then u clearly also satisfies (2.3). Solving (2.3), using $(\det A, r) = 1$, yields that $r \mid u_i$, $i = 1, 2, \ldots, n$. Set $u_i = ru'_i$. Then $|u'_i| < q_i$ and $u' = (u'_1, u'_2, \ldots, u'_n)^{\mathrm{T}}$ is a solution of (2.2). Since A is Q-regular, Lemma 2.1 requires $u'_i = 0$. So $u_i = 0$, $i = 1, 2, \ldots, n$, and, thus, A is rQ-regular.

Necessity: Now suppose that A is rQ-regular. In this case, if there is a nonzero solution of (2.2) $u' = (u'_1, u'_2, \ldots, u'_n)^{\mathrm{T}}$ with $|u'_i| < q_i$, $i = 1, 2, \ldots, n$, then we may obtain a nonzero solution of (2.1), $u = ru' = (ru'_1, ru'_2, \ldots, ru'_n)$ with $|u_i| < rq_i$, $i = 1, 2, \ldots, n$, contradicting the rQ-regularity of A. Therefore, there is no such u', and Lemma 2.1 yields that A is Q-regular, the first part of the condition. If $1 < (\det A, r)$, then there would exist $b = (b_1, b_2, \ldots, b_n)^{\mathrm{T}}$; $0 \leqslant b_i < r, 1 \leqslant i \leqslant n$ such that $Av \equiv b \pmod r$ would have no solution $v \in \mathscr{V}(r)$. Then, $Av \equiv b \pmod{rQ}$ could have no solution $v \in \mathscr{V}(rQ)$, contradicting the rQ-regularity of A. Therefore, $(\det A, r) = 1$. □

An additional lemma will be used to establish our main theorem.

Lemma 2.3. *Let $q_1, q_2, \ldots, q_n$ be any positive integers greater than unity, and let R_i be an arbitrarily selected complete residue system of the modulus q_i, $i = 1, 2, \ldots, n$. Then*

$$
\begin{aligned}
&R_1 + q_1 R_2 + \cdots + (q_1 \cdots q_{n-1}) R_n \\
&\quad = \{\rho_1 + q_1\rho_2 + \cdots + (q_1 \cdots q_{n-1})\rho_n \colon \rho_i \in R_i\}
\end{aligned}
$$

constitutes a complete residue system of the modulus $q_1 q_2 \cdots q_n$.

This lemma follows, for example, from $n - 1$ applications of the division algorithm [7, p. 23], but we omit the proof.

3. Regularity in a special case

The special case has $Q = (rq_1, rq_2, \ldots, rq_n)^{\mathrm{T}}$, with r any positive integer and $(q_i, q_j) = 1$ for $1 \leqslant i < j \leqslant n$. We introduce notation and derive elementary results before stating a theorem on Q-regularity for this case.

We employ a permutation matrix representation of the symmetric group of degree n, $\mathscr{S}_n$, which we assume acts upon the set $\{1, 2, \ldots, n\}$. For $\sigma \in \mathscr{S}_n$, let $\sigma(i)$ denote the element which i maps to under σ, $i = 1, 2, \ldots, n$. Consider also the corresponding (0–1)-*permutation matrix* of order n, with 1's only at the positions $(i, \sigma(i))$, $i = 1, 2, \ldots, n$ [1, p. 447].

Definition 3.1. For any vector $w = (w_1, w_2, \ldots, w_n)^{\mathrm{T}}$, and for any σ in $\mathscr{S}_n$, let P_σ denote the permutation matrix of order *n*, with the (conventional) matrix product $P_\sigma w = w_\sigma \overset{\text{def}}{=} (w_{\sigma(1)}, w_{\sigma(2)}, \ldots, w_{\sigma(n)})^{\mathrm{T}}$.

Note that the only matrix multiplications in our paper that are not performed modulo Q are the permutations induced by standard matrix multiplication with a permutation matrix. Thus, from the action of P_σ on vectors, $P_\sigma A P_\sigma^{\mathrm{T}}$ equals $[a_{\sigma(i)\,\sigma(j)}]$; $1 \leqslant i, j \leqslant n$; viz., Example 3.4. It is easily seen that $P_\sigma A P_\sigma^{\mathrm{T}}$ is a regularity-preserving transformation.

Remark 3.2. *For any σ in $\mathscr{S}_n$ and A in $M_n(\mathbb{Z})$, and for any vector Q of positive integers greater than unity, A is Q-regular if and only if $P_\sigma A P_\sigma^{\mathrm{T}}$ is Q_σ-regular.*

Proof. Clearly, $P_\sigma(Av \pmod{Q}) = P_\sigma A P_\sigma^{\mathrm{T}} v_\sigma \pmod{Q_\sigma}$. Therefore, both sides yield the same number of distinct vectors as v and v_σ range over $\mathscr{V}(Q)$ and $\mathscr{V}(Q_\sigma)$, respectively. □

Definition 3.3. Let A be in $M_n(\mathbb{Z})$, and let $Q = (q_1, q_2, \ldots, q_n)^{\mathrm{T}}$. Then A is called *lower* (*upper*) *Q-triangular* if, for each i and j in $\{1, 2, \ldots, n\}$, $q_i \mid a_{ij}$ whenever $j > i$ ($j < i$).

Example 3.4.

$$\sigma = (1\,3)(2\,4), \quad P_\sigma = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 1 & 1 & 3 & 1 \\ 1 & 2 & 0 & 1 \end{pmatrix}.$$

$$P_\sigma A P_\sigma^{\mathrm{T}} = \begin{pmatrix} 3 & 1 & 1 & 1 \\ 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix} \text{ (an upper triangular matrix).}$$

We now state a theorem on regularity for the special case.

Theorem 3.5. *Let $Q = (q_1, q_2, \ldots, q_n)^{\mathrm{T}}$ be a vector of pairwise coprime integers greater than unity, and let A be in $M_n(\mathbb{Z})$. Then A is rQ-regular if and only if both $(\det A, r) = 1$ and there exists a σ in $\mathscr{S}_n$ such that $P_\sigma A P_\sigma^{\mathrm{T}}$ is lower Q_σ-triangular and has each main diagonal element coprime to its respective modulus.*

Proof. Recall that $rQ = (rq_1, rq_2, \ldots, rq_n)^{\mathrm{T}}$. From Lemma 2.2, A is rQ-regular if and only if $(\det A, r) = 1$ and A is Q-regular. Therefore, it suffices to prove the theorem by demonstrating that A is Q-regular if and only if there is a $\sigma \in \mathscr{S}_n$ such that $P_\sigma A P_\sigma^{\mathrm{T}}$ is lower Q_σ-triangular and $(q_i, a_{ii}) = 1$, $i = 1, 2, \ldots, n$.

The sufficiency of the latter condition follows directly from Lemma 2.1 and Remark 3.2. We now prove its necessity by induction on n. Suppose that A is Q-regular. For $n=1$, this condition must hold [4, Theorem 57]. Assume that $n>1$ and that the condition holds for $n-1$.

Set $m = q_1 q_2 \cdots q_n$ and $m_i = m/q_i$, $i = 1, 2, \ldots, n$. By assumption, $(m_i, q_i) = 1$. There is, therefore, a unique $r_i \in Z_{q_i} \stackrel{\text{def}}{=} \{0, 1, \ldots, q_i - 1\}$ such that $m_i r_i \equiv 1 \pmod{q_i}$. Put $\alpha_i = m_i r_i$. Then

$$\alpha_i \equiv \begin{cases} 1 \pmod{q_i}, & \\ 0 \pmod{q_j}, & i \neq j. \end{cases} \tag{3.1}$$

From the Chinese remainder theorem (cf. [6, Theorem 1, p. 34] and [4, Theorem 121]), for any two n-sequences of integers $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$,

$$\alpha_1 a_1 + \alpha_2 a_2 + \cdots + \alpha_n a_n \equiv \alpha_1 b_1 + \alpha_2 b_2 + \cdots + \alpha_n b_n \pmod{m}$$

holds if and only if $a_i \equiv b_i \pmod{q_i}$, $i = 1, 2, \ldots, n$. Therefore, $\alpha_1 a_1 + \alpha_2 a_2 + \cdots + \alpha_n a_n \pmod{m}$ ranges over Z_m whenever all the a_i's range over the respective Z_{q_i}'s.

Let the indeterminates be denoted $v_1, v_2, \ldots, v_n$, and set

$$\begin{aligned} &\alpha_1(a_{11}v_1 + a_{12}v_2 + \cdots + a_{1n}v_n) + \alpha_2(a_{21}v_1 + a_{22}v_2 + \cdots + a_{2n}v_n) \\ &\quad + \cdots + \alpha_n(a_{n1}v_1 + a_{n2}v_2 + \cdots + a_{nn}v_n) \\ &\qquad = v_1(a_{11}\alpha_1 + a_{21}\alpha_2 + \cdots + a_{n1}\alpha_n) \\ &\qquad\quad + v_2(a_{12}\alpha_1 + a_{22}\alpha_2 + \cdots + a_{n2}\alpha_n) \\ &\qquad\quad + \cdots + v_n(a_{1n}\alpha_1 + a_{2n}\alpha_2 + \cdots + a_{nn}\alpha_n) \\ &\qquad = v_1 A_1 + v_2 A_2 + \cdots + v_n A_n, \end{aligned}$$

where

$$A_j \stackrel{\text{def}}{=} \alpha_1 a_{1j} + \alpha_2 a_{2j} + \cdots + \alpha_n a_{nj}, \quad j = 1, 2, \ldots, n.$$

We have the following corollary of the Chinese remainder theorem and Definition 1.1, which is central to the proof of the theorem.

Corollary 3.6. *When $(q_i, q_j) = 1$ for $1 \leqslant i < j \leqslant n$, A is Q-regular if and only if*

$$v_1 A_1 + v_2 A_2 + \cdots + v_n A_n \pmod{m}$$

ranges over Z_m when the v_i's range over the respective Z_{q_i}'s.

To complete the proof, define a character $\lambda(v)$ on Z_m as follows:

$$\lambda : v \longrightarrow \mathrm{e}^{2\pi v\sqrt{-1}/m}.$$

Clearly,

$$\lambda(v + w) = \lambda(v)\lambda(w). \tag{3.2}$$

Then, if A is regular,

$$\sum_{v_i \in Z_{q_i}\ (1 \leqslant i \leqslant n)} \lambda(v_1 A_1 + v_2 A_2 + \cdots + v_n A_n) = 0.$$

Because of (3.2), regularity of A implies that there is an index k with $1 \leqslant k \leqslant n$ such that

$$\sum_{v_k \in Z_{q_k}} \lambda(v_k A_k) = 0.$$

Set $\zeta = \lambda(A_k)$. Then, the foregoing equation gives

$$\zeta^{q_k} - 1 = (\zeta - 1)\left(1 + \zeta + \cdots + \zeta^{q_k - 1}\right) = 0,$$

from which it follows that $\zeta^{q_k} = 1$. ($\zeta \neq 1$ because $a_{kk} \not\equiv 0 \pmod{q_k}$.) This implies that m_k ($= m/q_k = \prod_{i \neq k} q_i$) divides $A_k = \alpha_1 a_{1k} + \alpha_2 a_{2k} + \cdots + \alpha_n a_{nk}$. From (3.1) it follows that, for $i \neq k$, $q_i \mid a_{ik}$, $1 \leqslant i \leqslant n$. Furthermore, the Q-regularity of A necessitates $(q_k, a_{kk}) = 1$ because $A_k \equiv a_{kk} \pmod{q_k}$. Thus, otherwise, if v_k were to range over Z_{q_k}, then the resulting $v_k A_k \pmod{q_k}$ would generate an incomplete residue system [4, Theorem 57].

Let τ denote the permutation $(k\ n)$, interchanging $k \in \{1, 2, \ldots, n\}$ with n and fixing the remaining elements of $\{1, 2, \ldots, n\}$, and consider $P_\tau A P_\tau^{\mathrm{T}}$. (If $k = n$, then τ is the identity.) Clearly, $q_{\tau(i)} | a_{\tau(i)\,\tau(k)}$ for all i in $\{1, 2, \ldots, n\} \backslash k$, and $(q_{\tau(k)}, a_{\tau(k)\tau(k)}) = 1$. Recall, from Remark 3.2, that A is Q-regular if and only if $P_\tau A P_\tau^{\mathrm{T}}$ is Q_τ-regular. From the form of $P_\tau A P_\tau^{\mathrm{T}}$, it is readily seen that this may hold if and only if the latter's leading submatrix of order $n - 1$, denoted B, is $(q_{\tau(1)}, q_{\tau(2)}, \ldots, q_{\tau(n-1)})$-regular. By the induction hypothesis, there exists a permutation $\omega \in \mathscr{S}_{n-1}$ of $(\tau(1), \tau(2), \ldots, \tau(n-1))$, acting on the indices of τ, such that $P_\omega B P_\omega^{\mathrm{T}}$ is lower Q_ω-triangular and $(q_{\tau(i)}, b_{ii}) = 1$, $i = 1, 2, \ldots, n - 1$. Let $\sigma \in \mathscr{S}_n$ denote the permutation of $\{1, 2, \ldots, n\}$ with $\sigma(i) = \omega(\tau(i))$, $i = 1, 2, \ldots, n - 1$, and $\sigma(n) = \tau(n) = k$. Then, $P_\sigma A P_\sigma^{\mathrm{T}}$ is clearly lower Q_σ-triangular and $(q_i, a_{ii}) = 1$, $i = 1, 2, \ldots, n$. □

Note that though our theorems are stated in terms of lower triangular matrices, lower and upper Q-triangular matrices are plainly interconvertible.

Remark 3.7. *An upper (lower) Q-triangular matrix A from $M_n(\mathbb{Z})$ is convertible into a lower (upper) Q_φ-triangular matrix $P_\varphi A P_\varphi^{\mathrm{T}}$, where $P_\varphi (= P_\varphi^{\mathrm{T}})$ denotes the permutation matrix with its 1's on its off diagonal and $\varphi = (1\ n)(2\ n-1)(3\ n-2)\cdots$.*

Proof. For instance, if A is lower Q-triangular, then $P_\varphi A P_\varphi^{\mathrm{T}} = [a_{\varphi(i)\,\varphi(j)}]$ is upper Q_φ-triangular because, with $\varphi : i \longrightarrow n + 1 - i$, $i = 1, 2, \ldots, n$, $j > i$ if and only if $\varphi(j) < \varphi(i)$, yielding $q_{\varphi(i)} \mid a_{\varphi(i)\,\varphi(j)}$ whenever $\varphi(j) < \varphi(i)$. □

Theorem 3.5 yields a complete description of Q-regular matrices of order 2. Let $Q = (q_1, q_2)^{\mathrm{T}}$, with $q_1 = rr_1$ and $q_2 = rr_2$, where $r = (q_1, q_2)$. Let

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M_2(\mathbb{Z}).$$

Corollary 3.8. *A 2×2 matrix A is Q-regular if and only if* $(r, \ \det \ A) = 1$, $(a_{11}, r_1) = (a_{22}, r_2) = 1$, *and either* $r_1 \mid a_{12}$ *or* $r_2 \mid a_{21}$ (*or both*).

4. Regularity-preserving transformations

In Section 3, we described some transformations preserving the regularity of linear systems of congruences (viz., Remark 3.2). For the foregoing transformations, Q_σ replaces Q. This section describes Q-regularity-preserving transformations in which Q is fixed. It also contains regularity-preserving transformations for particular transformations of Q which increase the number of its elements. Both classes of transformations are used to obtain fully general results on regularity, in Section 5.

In this section, we suppose that $Q = (q_1, q_2, \ldots, q_n)^{\mathrm{T}}$ is an arbitrary vector of integers greater than unity. Let $q_n = q_{n1}q_{n2}$ with $(q_{n1}, q_{n2}) = 1$. Set $\xi(Q) \stackrel{\text{def}}{=} (q_1, \ldots, q_{n-1}, q_{n1}, q_{n2})^{\mathrm{T}}$. From A in $M_n(\mathbb{Z})$, we obtain $\Xi(A)$ in $M_{n+1}(\mathbb{Z})$:

$$\Xi(A) \stackrel{\text{def}}{=} \begin{pmatrix} A & A_{\mathrm{c}}q_{n1} \\ A_{\mathrm{r}} & a_{nn}q_{n1} \end{pmatrix},$$

where A_{c} and A_{r} are the nth column and nth row of A, respectively.

Let v_n be an integer with $0 \leqslant v_n < q_n$. By the division algorithm [7, p. 23], there are unique $v_n^{(1)}$ and $v_n^{(2)}$, with $0 \leqslant v_n^{(1)} < q_{n1}$ and $0 \leqslant v_n^{(2)} < q_{n2}$, such that $v = v^{(1)} + q_{n1}v^{(2)}$. Thus, we obtain a bijection μ from $\mathscr{V}(Q)$ to $\mathscr{V}(\xi(Q))$ given by

$$\mu : (v_1, \ldots, v_{n-1}, v_n)^{\mathrm{T}} \longrightarrow \left(v_1, \ldots, v_{n-1}, v_n^{(1)}, v_n^{(2)}\right)^{\mathrm{T}}.$$

Proposition 4.1. *A is Q-regular if and only if $\Xi(A)$ is $\xi(Q)$-regular.*

Proof. Given $v = (v_1, v_2, \ldots, v_n)^{\mathrm{T}}$ with $|v_i| < q_i$, $i = 1, 2, \ldots, n$, we transform v according to ν:

$$\nu(v) = \begin{cases} \left(v_1, \ldots, v_{n-1}, v_n^{(1)}, v_n^{(2)}\right) & \text{if } 0 \leqslant v_n, \\ \left(v_1, \ldots, v_{n-1}, -|v_n|^{(1)}, -|v_n|^{(2)}\right) & \text{if } v_n < 0, \end{cases}$$

using the foregoing division algorithm to obtain either $v_n^{(1)}$ and $v_n^{(2)}$, if $0 \leqslant v_n$ or $|v_n|^{(1)}$ and $|v_n|^{(2)}$, otherwise. Then it is easy to see that v is the zero vector in $\mathscr{V}(Q)$ if and only if $\nu(v)$ is the zero vector in $\mathscr{V}(\xi(Q))$.

Now, we claim that $Av \equiv 0 \pmod{Q}$ if and only if $\Xi(A)\nu(v) \equiv 0 \pmod{\xi(Q)}$. In fact, for given v and A, and with $0 \leqslant v_n$,

$$\Xi(A)\nu(v)=\begin{pmatrix} a_{11}v_1+\cdots+a_{1n-1}v_{n-1}+a_{1n}v_n^{(1)}+a_{1n}q_{n1}v_n^{(2)} \\ a_{21}v_1+\cdots+a_{2n-1}v_{n-1}+a_{2n}v_n^{(1)}+a_{2n}q_{n1}v_n^{(2)} \\ \vdots \\ a_{n1}v_1+\cdots+a_{nn-1}v_{n-1}+a_{nn}v_n^{(1)}+a_{nn}q_{n1}v_n^{(2)} \\ a_{n1}v_1+\cdots+a_{nn-1}v_{n-1}+a_{nn}v_n^{(1)}+a_{nn}q_{n1}v_n^{(2)} \end{pmatrix}$$

$$=\begin{pmatrix} a_{11}v_1+\cdots+a_{1n-1}v_{n-1}+a_{1n}v_n \\ a_{21}v_1+\cdots+a_{2n-1}v_{n-1}+a_{2n}v_n \\ \vdots \\ a_{n1}v_1+\cdots+a_{nn-1}v_{n-1}+a_{nn}v_n \\ a_{n1}v_1+\cdots+a_{nn-1}v_{n-1}+a_{nn}v_n \end{pmatrix}.$$

Our claim is immediately verified because, with $(q_{n1}, q_{n2}) = 1$, $a_{n1}v_1 + \cdots + a_{nn-1}v_{n-1} + a_{nn}v_n \equiv 0 \pmod{q_{ni}}$, $i = 1, 2$, hold if and only if $a_{n1}v_1 + \cdots + a_{nn-1}v_{n-1} + a_{nn}v_n \equiv 0 \pmod{q_n}$. Analogous results clearly obtain when $v_n < 0$. Thus, the proposition follows immediately from Lemma 2.1. □

The following corollary may be used in the solution of regular systems.

Corollary 4.2. *Given $b \in \mathscr{V}(Q)$, with $q_n = q_{n1}q_{n2}$ and $(q_{n1}, q_{n2}) = 1$, and $A \in M_n(\mathbb{Z})$, we may obtain a solution $x \in \mathscr{V}(Q)$ for the system of congruences $Ax \equiv b \pmod{Q}$ from that of $\Xi(A)x' \equiv b' \pmod{\xi(Q)}$, with $b'(i) = b(i)$, $i = 1, 2, \ldots, n-1$, $b'(n) \equiv b(n) \pmod{q_{n1}}$, and $b'(n+1) \equiv b(n) \pmod{q_{n2}}$ as follows: $x = \mu^{-1}(x')$, with μ denoting the foregoing bijection.*

As a consequence of Proposition 4.1, we need to resolve regularity only for the case with $Q = (p_1^{e_1}, p_2^{e_2}, \ldots, p_n^{e_n})^{\mathrm{T}}$, where the p_i's are primes (not necessarily distinct) and the e_i's are positive integers. When Q contains different moduli, standard transformations of matrices [5, vol. 6, p. 470] are not guaranteed to preserve Q-regularity. We have the following proposition.

Proposition 4.3. *Let $Q = (q_1, q_2, \ldots, q_n)^{\mathrm{T}}$ be a vector of integers greater than unity, and let A in $M_n(\mathbb{Z})$ be Q-regular. Then, the following transformations of A preserve its Q-regularity, with $\alpha \in \mathbb{N}$:*

(I) *The addition of an α-multiple of the* ith *row to the* jth *row if $q_j | \alpha q_i$, $1 \leqslant i, j \leqslant n$; $i \neq j$.*
(II) *The replacement of the* ith *row by its α-multiple if $(\alpha, q_i) = 1$, $1 \leqslant i \leqslant n$.*
(III) *The interchange of the* ith *and* jth *rows (or columns) if $q_i = q_j$, $1 \leqslant i, j \leqslant n$.*

(IV) *Replacement of the elements of the* ith *row by their respective residues modulo* q_i, $1 \leqslant i \leqslant n$.

Note that (I), (II), and (III) generalize the conventional transformations of rows—(1), (2), and (3) of [5, vol. 5, p. 472], respectively. Note also that, of the three conventional column transformations, only (III) is retained. The proofs that transformations (II), (III), and (IV) preserve the Q-regularity of A follow immediately from their definitions.

Proof (*of transformation* (I)). Let $T_{ij}(\alpha)$ denote such a transformation matrix. In order to prove the assertion, by Lemma 2.1, it suffices to show that the congruence systems

$$Av \equiv 0 \ (\mathrm{mod}\ Q) \tag{4.1}$$

and

$$T_{ij}(\alpha)Av \equiv 0 \ (\mathrm{mod}\ Q) \tag{4.2}$$

have the same solutions of the form $v = (v_1, v_2, \ldots, v_n)^{\mathrm{T}}$, with $|v_l| < q_l$, $l = 1, 2, \ldots, n$.

It is seen that the two systems consist of the same congruences except for the jth, which are, respectively,

$$A_{j\cdot}v \equiv 0 \ (\mathrm{mod}\ q_j) \tag{4.3}$$

and

$$(A_{j\cdot} + \alpha A_{i\cdot})v \equiv 0 \ (\mathrm{mod}\ q_j), \tag{4.4}$$

where $A_{i\cdot}$ and $A_{j\cdot}$ denote the ith and jth rows of A, respectively. From this and the condition $q_j \mid \alpha q_i$, the assertion is immediately verified. □

Definition 4.4. Let $Q = (q_1, q_2, \ldots, q_n)^{\mathrm{T}}$ be a vector of integers greater than unity, and let A and B be in $M_n(\mathbb{Z})$. If B is obtainable from A by a series of the elementary transformations listed in Proposition 4.3, then we say A and B are Q-*equivalent*.

Example 4.5. Consider the system

$$\begin{pmatrix} 1 & 2 \\ 5 & 3 \end{pmatrix} \mathrm{mod} \begin{pmatrix} 24 \\ 26 \end{pmatrix}.$$

Corollary 3.8 establishes the non-regularity of this system. However, this example also illustrates the applicability of the results of this section and introduces the results of Section 5.

First, factor the modulus 26 into its prime factors, applying Proposition 4.1, yielding the equivalent system

$$\begin{pmatrix} 1 & 0 & 1 \\ 3 & 6 & 5 \\ 2 & 4 & 1 \end{pmatrix} \bmod \begin{pmatrix} 2 \\ 13 \\ 24 \end{pmatrix}.$$

Here we used transformation (IV) and $P_{(1\,2\,3)}$ and its transpose to permute the resulting system. Another application of Proposition 4.1, to factor the modulus 24 into prime-power factors, yields the equivalent system

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 1 & 0 & 1 \\ 2 & 1 & 3 & 4 \\ 3 & 5 & 2 & 6 \end{pmatrix} \bmod \begin{pmatrix} 2 \\ 3 \\ 8 \\ 13 \end{pmatrix}.$$

The final system is evidently not convertible into lower triangular form by the transformations of Proposition 4.3. For instance, though adding row 3 to row 1 yields $(1, 0, 0, 0)$ for the latter (mod 2), ultimately, insufficiently many zeroes may be generated. As will be seen in the subsequent section, Theorem 5.1 establishes that this convertibility is necessary for all regular systems, when the moduli are prime powers.

5. General resolution of regularity

From Proposition 4.1, an arbitrary $A \in M_n(\mathbb{Z})$ and a vector of moduli Q yield a corresponding $A' \in M_{n'}(\mathbb{Z})$, with $n \leqslant n'$ and a vector of moduli Q', with the elements of Q' being (not necessarily distinct) prime powers. In this section, we determine the necessary and sufficient conditions for the derived system to be regular. (Henceforth, we omit the superscript '$'$'.)

Theorem 5.1. *Let $Q = (q_1, q_2, \ldots, q_n)^{\mathrm{T}}$ be a vector of positive integral powers of primes, and let A be in $M_n(\mathbb{Z})$. Then A is Q-regular if and only if there exists a $\sigma \in \mathscr{S}_n$ with $P_\sigma A P_\sigma^{\mathrm{T}}$ Q_σ-equivalent to a lower triangular matrix, having each main diagonal element coprime to its respective modulus from Q_σ.*

Proof. *Sufficiency*: Given a lower triangular matrix $T \in M_n(\mathbb{Z})$ whose main diagonal elements are coprime to their respective modulus, from Q_σ, and, also, given any $b = (b_1, b_2, \ldots, b_n)^{\mathrm{T}} \in \mathscr{V}(Q_\sigma)$, we may invert the system

$$Tx \equiv b \pmod{Q_\sigma}$$

for a unique $x = (x_1, x_2, \ldots, x_n)^{\mathrm{T}} \in \mathscr{V}(Q_\sigma)$. This is established by noting that because the diagonal elements of T, t_{ii}, satisfy $(q_{\sigma(i)}, t_{ii}) = 1$, one may sequentially solve each congruence for a unique x_i, starting with x_1 (cf. [4, Theorem 57]). It follows that T is Q_σ-regular because, for instance, were x the solution for two different b's, say b_α and b_β, then $b_\alpha \equiv b_\beta \pmod{Q_\sigma}$. Therefore, because a series of regularity-preserving transformations yields a regular, triangular system, A is established to be Q-regular.

Necessity: From Proposition 4.3 (IV), it may be assumed that $0 \leqslant a_{ij} < q_i$, $i, j = 1, 2, \ldots, n$. Using (III), it may also be assumed that $q_1, q_2, \ldots, q_{r_1}$ are powers of the prime p_1; $q_{r_1+1}, q_{r_1+2}, \ldots, q_{r_1+r_2}$ are powers of the prime p_2;...; and $q_{r_1+\cdots+r_{\ell-1}+1}$, $q_{r_1+\cdots+r_{\ell-1}+2}, \ldots, q_{r_1+\cdots+r_{\ell-1}+r_\ell}$ are powers of the prime p_ℓ. Thus, $r_1 + \cdots + r_\ell = n$. Let $r_0 = 0$. Then, let

$$P_i = q_{r_0+\cdots+r_{i-1}+1} q_{r_0+\cdots+r_{i-1}+2} \cdots q_{r_0+\cdots+r_{i-1}+r_i}, \quad i = 1, 2, \ldots, \ell,$$

and let $M = \prod_{i=1}^{n} q_i = \prod_{j=1}^{\ell} P_j$. Then, from the Chinese remainder theorem, there are positive integers $\beta_1, \beta_2, \ldots, \beta_\ell$ such that

$$\beta_i \equiv \begin{cases} 1 \pmod{P_i}, \\ 0 \pmod{P_j}, \quad j \neq i. \end{cases} \tag{5.1}$$

Also, for $1 \leqslant i \leqslant \ell$, define $P_i^{(1)} = 1$ and

$$P_i^{(j)} = \prod_{h=1}^{j-1} q_{r_0+r_1+\cdots+r_{i-1}+h}, \quad j = 2, 3, \ldots, r_i, \; i = 1, 2, \ldots, \ell.$$

Let $A_{i\cdot} = (a_{i1}, a_{i2}, \ldots, a_{in})$, and take $v = (v_1, v_2, \ldots, v_n)^{\mathrm{T}} \in \mathscr{V}(Q)$. Then, after making transformations of type (II), using Lemma 2.3, it follows from the Chinese remainder theorem and Corollary 3.6 that

$$\begin{aligned}
&\left(P_1^{(1)} A_{1\cdot} v + P_1^{(2)} A_{2\cdot} v + \cdots + P_1^{(r_1)} A_{r_1\cdot} v\right)\beta_1 \\
&\quad + \left(P_2^{(1)} A_{r_1+1\cdot} v + P_2^{(2)} A_{r_1+2\cdot} v + \cdots + P_2^{(r_2)} A_{r_1+r_2\cdot} v\right)\beta_2 \\
&\quad + \cdots + \left(P_\ell^{(1)} A_{r_1+\cdots+r_{\ell-1}+1\cdot} v + P_\ell^{(2)} A_{r_1+\cdots+r_{\ell-1}+2\cdot} v \right. \\
&\quad \left. + \cdots + P_\ell^{(r_\ell)} A_{r_1+\cdots+r_\ell\cdot} v\right)\beta_\ell \\
&\quad\quad = B_1 v_1 + B_2 v_2 + \cdots + B_n v_n
\end{aligned}$$

must range over a complete residue system modulo M when v ranges over $\mathscr{V}(Q)$, where

$$\begin{aligned}
B_j \stackrel{\text{def}}{=} &\left(P_1^{(1)} a_{1j} + P_1^{(2)} a_{2j} + \cdots + P_1^{(r_1)} a_{r_1 j}\right)\beta_1 \\
&+ \left(P_2^{(1)} a_{(r_1+1)j} + P_2^{(2)} a_{(r_1+2)j} + \cdots + P_2^{(r_2)} a_{(r_1+r_2)j}\right)\beta_2 \\
&+ \cdots + \left(P_\ell^{(1)} a_{(r_1+\cdots+r_{\ell-1}+1)j} + P_\ell^{(2)} a_{(r_1+\cdots+r_{\ell-1}+2)j} \right. \\
&\left. + \cdots + P_\ell^{(r_\ell)} a_{(r_1+\cdots+r_\ell)j}\right)\beta_\ell, \quad j = 1, 2, \ldots, n.
\end{aligned} \tag{5.2}$$

As in the proof of Theorem 3.5, the character λ on Z_M establishes the existence of an index k, $1 \leqslant k \leqslant n$, for which M/q_k divides B_k. Without loss of generality, we assume that $1 \leqslant k \leqslant r_1$. It follows from (5.1), (5.2), and Lemma 2.3 that $a_{ik} = 0$ for $i > r_1$. Therefore,

$$\begin{aligned} &P_1^{(1)} a_{1k} + P_1^{(2)} a_{2k} + \cdots + P_1^{(r_1)} a_{r_1 k} \\ &\quad = a_{1k} + q_1 a_{2k} + \cdots + (q_1 q_2 \cdots q_{r_1 - 1}) a_{r_1 k} \\ &\quad \equiv 0 \ (\mathrm{mod}\ P_1/q_k). \end{aligned}$$

Recall that $q_1 = p_1^{e_1}, q_2 = p_1^{e_2}, \ldots, q_{r_1} = p_1^{e_{r_1}}$ and take $e_1 \geqslant e_2 \geqslant \cdots \geqslant e_{r_1}$. From this and the preceding congruence it follows that if $i < k$, then $q_i | a_{ik}$, yielding $a_{ik} = 0$. If $k = r_1$, then each entry of the kth column vanishes except for a_{kk}. Regularity implies that $(q_k, a_{kk}) = 1$. If, on the other hand, $k < r_1$, then we may construct a vector $\tilde{v} = (\tilde{v}_1, \tilde{v}_2, \ldots, \tilde{v}_n)^{\mathrm{T}} \in \mathscr{V}(Q)$, with $\tilde{v}_k = p_1^{e_k - 1}$ and $\tilde{v}_j = 0$ for $j \neq k$. Because $p_1 \,|\, a_{kk}$, we may write

$$A\tilde{v} \equiv (0, \ldots, 0, a_{(k+1)k} p_1^{e_k - 1}, \ldots, a_{r_1 k} p_1^{e_k - 1}, 0, \ldots, 0)^{\mathrm{T}} \ (\mathrm{mod}\ Q).$$

Since $\tilde{v}$ is not a zero vector and A is regular, Lemma 2.1 ensures that there is a j, with $k < j \leqslant r_1$, for which

$$a_{jk} p_1^{e_k - 1} \not\equiv 0 \left(\mathrm{mod}\ p_1^{e_j}\right),$$

implying that $e_j = e_k$ and $(a_{jk}, p_1) = 1$. Interchanging the kth and jth rows and performing a series of elementary transformations of type (I), of Proposition 4.3, transforms A into a matrix with $(q_k, a_{kk}) = 1$ and all other elements of the kth column equal zero (cf. [4, Theorem 57]). Now that we have established a column of zeroes, except for its diagonal element, we may employ the inductive part of the proof of Theorem 3.5 to establish the necessity of the asserted properties for all n. $\square$

Definition 5.2. Let Q be a vector of integers greater than unity and let $\Delta_n^*(Q)$ denote the lower triangular matrices from $M_n(\mathbb{Z})$ whose diagonal elements are nonzero and coprime to their respective modulus and whose elements d_{ij} satisfy $0 \leqslant d_{ij} < q_i, \ j = 1, 2, \ldots, i, \ i = 1, 2, \ldots, n$.

As a corollary of the proof of sufficiency for Theorem 5.1, we have:

Corollary 5.3. *Given A and $B \in \Delta_n^*(Q)$, the matrix congruence $AX \equiv B$ (mod Q) has a unique solution $X \in \Delta_n^*(Q)$.*

On the other hand, evidently, $YA \equiv B \ (\mathrm{mod}\ Q)$ may have no solution $Y \in \Delta_n^*(Q)$—nor need solutions be unique.

Acknowledgements

This work was done under the auspices of the US Department of Energy, under Contract W-7405-ENG-36, and the Center for Nonlinear Studies of Los Alamos National Laboratory. Jun Wang was also supported by the Li Foundation, the National Natural Science Foundation of China (Grant No. 19831050), and the Natural Science Foundation of Liaoning Province of China. We are very grateful to the anonymous referee for their comprehensive and incisive contributions to the exposition and accuracy of our results. Finally, the authors are indebted to Dr. William Y.C. Chen, of Nankai University, for initiating the collaboration on the topic of this paper.

References

[1] E.J. Borowski, J.M. Borwein, The HarperCollins Dictionary of Mathematics, HarperCollins Publishers, New York, 1991.
[2] A.T. Butson, B.M. Stewart, Systems of linear congruences, Canad. J. Math. 7 (1955) 358–368.
[3] H.S.M. Coxeter, Regular Polytopes, Dover, New York, 1973.
[4] G.H. Hardy, E.M. Wright, An Introduction to the Theory of Numbers, fifth ed., Clarendon Press, Oxford, 1984, pp. 51, 52.
[5] M. Hazewinkel (Ed.), Encyclopædia of Mathematics, Kluwer Academic Publishers, Dordrecht, 1990.
[6] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, Springer, New York, 1982.
[7] N. Jacobson, Basic Algebra I, 2nd ed., Freeman, San Francisco, CA, 1985.