Greatest Common Divisor Matrices

Scott Beslin and Steve Ligh
Department of Mathematics
University of Southwestern Louisiana
Lafayette, Louisiana 70504

Submitted by Robert Hartwig

ABSTRACT

Let $S = \{x_1, x_2, \ldots, x_n\}$ be a set of distinct positive integers. The $n \times n$ matrix $[S] = (s_{ij})$, where $s_{ij} = (x_i, x_j)$, the greatest common divisor of x_i and x_j, is called the greatest common divisor (GCD) matrix on S. We initiate the study of GCD matrices in the direction of their structure, determinant, and arithmetic in Z_n. Several open problems are posed.

1. INTRODUCTION

Let $S = \{x_1, x_2, \ldots, x_n\}$ be a set of distinct positive integers. The $n \times n$ matrix $[S] = (s_{ij})$, where $s_{ij} = (x_i, x_j)$, the greatest common divisor of x_i and x_j, is called the greatest common divisor (GCD) matrix on S. In this paper we initiate the study of GCD matrices. We shall obtain a structure theorem for GCD matrices and show that each is positive definite and hence nonsingular. A corollary of our result yields a different proof and a generalization of the so-called Smith's determinant [9]. We shall also consider GCD matrices with arithmetic in Z_n, integers modulo n.

While we have obtained some very interesting properties of GCD matrices, there remain many unanswered questions about them. Our conjectures and open problems will provide a direction for further study of GCD matrices.

655 Avenue of the Americas, New York, NY 10010 0024-3795/89/$3.50

2. GCD MATRICES AND DETERMINANTS

DEFINITION 1. Let $S = \{x_1, x_2, \ldots, x_n\}$ be a set of distinct positive integers. The $n \times n$ matrix $[S] = (s_{ij})$, where $s_{ij} = (x_i, x_j)$, the greatest common divisor of x_i and x_j, is called the greatest common divisor (GCD) matrix on S.

In this section we initiate the study of GCD matrices. H.J.S. Smith [9] considered the determinant of the GCD matrix defined on the set $\{1, 2, \ldots, n\}$. Clearly GCD matrices are symmetric, and in fact, we shall show that each can be written as a product of A and A^T, the transpose of A, for some matrix A.

DEFINITION 2. A set S of positive integers is said to be factor-closed (FC) is whenever x_i is in S and d divides x_i, then d is in S.

The above definition is due to J. J. Malone.

It is clear that any set of positive integers is contained in an FC set. The following result describes the structure of GCD matrices.

THEOREM 1. *Let $S = \{x_1, x_2, \ldots, x_n\}$ be a set of distinct positive integers. Then the GCD matrix $[S]$ is the product of an $n \times m$ matrix A and the $m \times n$ matrix A^T, where the nonzero entries of A are of the form $\sqrt{\phi(d)}$ for some d in an FC set that contains S, and $\phi(x)$ is Euler's totient function.*

Proof. Suppose $D = \{d_1, d_2, \ldots, d_m\}$ is an FC set containing S. Let the matrix $A = (a_{ij})$ be defined as follows:

$$a_{ij} = e_{ij}(\lambda_j)^{1/2},$$

where

$$e_{ij} = \begin{cases} 1 & \text{if } d_j \text{ divides } x_i, \\ 0 & \text{otherwise,} \end{cases}$$

and $\lambda_j = \phi(d_j)$. Hence A is $n \times m$ and A^T is $m \times n$. Furthermore,

$$\begin{aligned}(AA^T)_{ij} &= \sum_{k=1}^{m} a_{ik}a_{jk} \\ &= \sum_{\substack{d_k \mid x_i \\ d_k \mid x_j}} \sqrt{\phi(d_k)}\sqrt{\phi(d_k)} \\ &= \sum_{d_k \mid (x_i, x_j)} \phi(d_k) \\ &= (x_i, x_j) \\ &= s_{ij}.\end{aligned}$$

Thus $[S] = AA^T$.

REMARK 1. Let E be the $n \times m$ matrix (e_{ij}) in Theorem 1, and let Λ be the $m \times m$ diagonal matrix with diagonal $(\lambda_1, \lambda_2, \ldots, \lambda_m) = (\phi(d_1), \phi(d_2), \ldots, \phi(d_m))$. Then $AA^T = (E \cdot \Lambda^{1/2})(E \cdot \Lambda^{1/2})^T = E\Lambda E^T$.

REMARK 2. Let $S = \{x_1, x_2, \ldots, x_n\}$, and let $S' = \{x_{i_1}, x_{i_2}, \ldots, x_{i_n}\}$ be the rearrangement of the elements of S so that $x_{i_1} < x_{i_2} < \cdots < x_{i_n}$. Then the GCD matrix $[S']$ is similar to $[S]$. Hence $\operatorname{rank}[S] = \operatorname{rank}[S']$ and $\det[S] = \det[S']$.

An immediate corollary of Theorem 1 and the fact that AA^T is nonnegative definite is the following result.

COROLLARY 1. *A GCD matrix* $[S]$ *is nonnegative definite.*

It is a pleasant surprise that each GCD matrix is nonsingular. This result follows from the next theorem.

THEOREM 2. *If* $[S]$ *is the GCD matrix defined on* $S = \{x_1, x_2, \ldots, x_n\}$, *then* $[S]$ *is positive definite.*

Proof. We prove that $\operatorname{rank}[S] = n$. By Remark 2, we may assume $x_1 < x_2 < \cdots < x_n$. From Theorem 1 and Remark 1, $[S] = AA^T = E\Lambda E^T$.

The set D in Theorem 1 may be chosen so that $d_1 = x_1$, $d_2 = x_2, \ldots,$ $d_n = x_n$. Hence $E = [E_1, E_2]$, where E_1 is an $n \times n$ lower triangular matrix of the form

$$\begin{bmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ * & & & 1 \end{bmatrix}.$$

Thus $\operatorname{rank}(E) = \operatorname{rank}(A) = \operatorname{rank}(AA^T) = n$. ■

It follows from Theorem 2 that the determinant of a GCD matrix $[S]$ is positive.

REMARK 3. Theorem 2 may also be obtained by noting the inequality $(x_i, x_j) \leq \sqrt{x_i x_j} \leq (x_i + x_j)/2$, which may be used to show that $u^T[S]u$ is positive for all nonzero $n \times 1$ column vectors u with real entries.

Our study of GCD matrices was motivated by the so-called Smith's determinant. In 1876, H. J. S. Smith [9] showed that the determinant of the GCD matrix $[E(n)]$ defined on $E(n) = \{1, 2, \ldots, n\}$ is, surprisingly, $\phi(1)\phi(2)\ldots\phi(n)$, where $\phi(m)$ is Euler's totient function. He also commented in that same paper that the above result remains valid if $E(n)$ is replaced by an FC set. Since then various generalizations and proofs [1, 6, 7] have been published. Smith's result can be obtained as a corollary of Theorem 1.

COROLLARY 2 (Smith [9]). *Let* $S = \{x_1, x_2, \ldots, x_n\}$ *be an FC set, and let* $[S]$ *be the GCD matrix defined on* S. *Then* $\det[S] = \phi(x_1)\phi(x_2)\cdots\phi(x_n)$.

Proof. Since S is an FC set from the proof of Theorem 1, take $D = S$ and $S = AA^T$, where A and A^T are lower triangular and upper triangular, respectively. Furthermore, $a_{ii} = \sqrt{\phi(x_i)} = (A^T)_{ii}$ for $i = 1, 2, \ldots, n$. Hence $\det[S] = \det(AA^T) = \det(A)\det(A^T) = \phi(x_1)\phi(x_2)\cdots\phi(x_n)$. ■

COROLLARY 3. *If* $E(n) = \{1, 2, \ldots, n\}$, *then* $\det[E(n)] = \phi(1)\phi(2)\cdots\phi(n)$.

We have considered the converse of Corollary 2 and believe that it is true, but we have not yet obtained a proof. We want to state it as a conjecture.

CONJECTURE 1. Let $T = \{t_1, t_2, \ldots, t_n\}$ be a set of distinct positive integers. If the determinant of the GCD matrix $[T]$ defined on T is $\phi(t_1)\phi(t_2)\cdots\phi(t_n)$, then T is an FC set.

Note that an FC set generalizes the set $E(n)$ as defined in Corollary 3. In a different direction, we considered another generalization of the set $E(n)$. Let $D(s,d,n)$ be the arithmetic progression defined as follows:

$$D(s,d,n) = \{s, s+d, s+2d, \ldots, s+(n-1)d\}$$

where $(s,d) = 1$.

Observe that $D(1,1,n) = E(n)$. The following open problem is mentioned in [5]:

PROBLEM 1. What is the value of the determinant of the GCD matrix defined on $D(s,d,n)$?

REMARK 4. While $\phi(n)$ gives the number of elements in $E(n)$ that are relatively prime to n, there is a function $\phi_d(n)$ described in [3,4] that gives the number of elements in $D(s,d,n)$ that are relatively prime to n. We conjecture that the function $\phi_d(n)$ plays an important role in Problem 1. Of course, if $D(s,d,n)$ is also an FC set, then Corollary 2 gives the value of the determinant. In fact, we have a complete characterization of arithmetic progressions that are also FC sets. We omit the proof.

THEOREM 3. *The arithmetic progression $D(s,d,n)$ is an FC set if and only if*

(i) $s = 1$, $d = 1$; $D(s,d,n) = E(n)$; *or*

(ii) $s = 1$, $d = 2$; $D(s,d,n) = \{1,3,5,7,\ldots,2n-1\}$; *or*

(iii) $D(s,d,n)$ *is a progression of primes* $\{1, p_1, p_2, \ldots\}$ *with* $|D(s,d,n)| \leqslant p_1 + 2$, *e.g.*, $\{1,37,73,109\}$, $\{1,31,61\}$, *and* $\{1,19,37\}$.

Finally, we ambitiously state the following problem.

PROBLEM 2. Let $S = \{x_1, x_2, \ldots, x_n\}$ be a set of distinct positive integers. What is the value of the determinant of the GCD matrix $[S]$?

REMARK 5. Because $[S]$ is positive definite, there is a bound on $\det[S]$: $\det[S] \leqslant x_1 x_2 \cdots x_n$.

3. GCD MATRICES (mod n)

In this section we consider GCD matrices defined on $E(n) = \{1,2,3,\ldots,n\}$ with arithmetic in Z_n, integers modulo n.

LEMMA 1. *Let $E(n) = \{1,2,\ldots,n\}$. For the following canonical forms of n, the determinant of the GCD matrix, $\det[E(n)]$, is congruent to zero* (mod n):

(1) $n = p_1^{a_1}p_2^{a_2}\ldots p_i^{a_i}$, $a_j > 1$ *for all j, and n is divisible by at least two distinct primes.*

(2) $n = 2^a$, $a \geq 2$.

(3) $n = p^a$, $a \geq 3$, p *an odd prime.*

(4) $n = 2p_1^{a_1}\cdots p_i^{a_i}$, $a_j > 1$ *for all j.*

Proof. (1): $p_j^{a_j}$ is in $E(n)$ for $j = 1,2,\ldots,i$, and $p_1^{a_1}p_j^{a_j}$ is in $E(n)$ for $j = 2,3,\ldots,i$. Now $\phi(p_j^{a_j})$ has a factor $p_j^{a_j-1}$. Also, $\phi(p_1^{a_1}p_j^{a_j})$ has a factor $p_1^{a_1-1}p_j^{a_j-1}$. Hence $\det[E(n)] = \prod_{x\in E(n)}\phi(x)$ has a factor $p_j^{(a_j-1)+(a_j-1)} = p_j^{2a_j-2} \geq p_j^{a_j}$ for all j, since $a_j \geq 2$. Thus $p_j^{a_j}$ divides $\det[E(n)]$ for all j and hence n divides $\det[E(n)]$.

(2): For $a = 2$, $\phi(1)\phi(2)\phi(3)\phi(4) = 4 \equiv 0$ (mod 4). For $a \geq 3$, 2^2 and 2^a are in $E(n)$. But 2 divides $\phi(2^2)$ and 2^{a-1} divides $\phi(2^a)$. Thus 2^a divides $\det[E(n)]$.

(3): Similar to (2), since p^2 and p^a are in $E(n)$.

(4): For all $j = 1,2,\ldots,i$, $p_j^{a_j}$ and $2p_j^{a_j}$ are in $E(n)$. The proof then follows as in (1). ∎

For certain values of n, the GCD matrices defined on $E(n)$ always have nonzero determinants.

LEMMA 2. *For $n = p$, p a prime, or for $n = 2p$, p an odd prime, $\det[E(n)]$ is not congruent to zero* (mod n).

Proof. The product $\phi(1)\phi(2)\cdots\phi(n) = \det[E(n)]$ is not congruent to zero (mod n) when $n = p$ or $n = 2p$, because in the former case, Z_p is a field, and in the latter case, there does not exist x in Z_n such that $\phi(x) = p$. ∎

Unlike the above values of n, the following result tells us that $\det[E(n)]$ may or may not be zero (mod n).

REMARK 6. In each of the values of n below, $\det[E(n)]$ may or may not be zero (mod n).

(1) *n has square-free odd prime factors.* For example, $\det[E(6)] \equiv 2 \pmod 6$, and $\det[E(15)] \equiv 0 \pmod{15}$.

(2) *$n = p^2$, p an odd prime.* Here we cannot find an example where $\det[E(n)]$ is not congruent to zero (mod n).

REMARK 7. For all primes p, $7 \leqslant p \leqslant 41$, there exist two values of k between 1 and p such that $1 + kp$ is a prime. Thus $\phi(1 + kp) = kp$, and $\det[E(n)]$ is congruent to zero (mod p^2). Since $\{1 + kp\}$, $k = 0, 1, 2, \ldots$, is a Dirichlet progression, there exist infinitely many primes of the form $1 + kp$. But does a prime occur for $1 \leqslant k < p$?

REMARK 8. The problem of determining exactly when $\det[E(n)]$ is congruent to zero (mod n) for $n = p^2$ or for n having an odd square-free part relates to the problem of finding solutions x to equations of the form $\phi(x) = m$ for specified values of m. In general, such equations are difficult to solve; some have no solutions (e.g., $m = 14$, $m = 26$).

Summarizing the above, we have the following result. The ring of $m \times m$ matrices over Z_n is denoted by $M_m(Z_n)$.

THEOREM 4. *The GCD matrix $[E(n)]$ is singular in $M_n(Z_n)$ when n has one of the forms* (1), (2), (3), *and* (4) *listed in Lemma* 1. *When $n = p$, a prime, the GCD matrix $[E(m)]$ is nonsingular in $M_m(Z_p)$ for $m = 1, 2, \ldots, n$.*

Finally, we state, without proof, other values of n for which the GCD matrix $[E(n)]$ is singular even though $\det[E(n)]$ may not be zero, since Z_n is a commutative ring and not a field.

THEOREM 5. *Suppose n has at least one square prime-power divisor p^2. If $p^2 \leqslant m \leqslant n$, then the GCD matrix $[S]$ is singular in $M_m(Z_n)$, where $S = \{1, 2, \ldots, m\}$.*

THEOREM 6. *Let $n = p_1 p_2 \cdots p_i$ be odd square-free with $i \geqslant 2$, and $p_1 < p_2 < \cdots < p_i$. If $p_1^2 \leqslant m \leqslant n$, then $[S]$ is singular in $M_m(Z_n)$, where $S = \{1, 2, \ldots, m\}$.*

COROLLARY 4. *If* $S = \{1,2,\ldots,n\}$, *then the GCD matrix* $[S]$ *is nonsingular in* $M_n(Z_n)$ *if and only if* n *is a prime.*

The authors are grateful to the editor and the referees for their valuable comments. In particular, Remark 3 is due to the editor.

REFERENCES

1 T. M. Apostol, Arithmetical properties of generalized Ramanujan sums, *Pacific J. Math.* 41:281–293 (1972).
2 G. Birkhoff and S. MacLane, *A Survey of Modern Algebra*, MacMillan, New York, 1965.
3 P. G. Garcia and S. Ligh, A generalization of Euler's ϕ-function, *Fibonacci Quart.* 21:26–28 (1983).
4 S. Ligh and P. G. Garcia, A generalization of Euler's ϕ-function, II, *Math. Japon.* 30:519–522 (1985).
5 S. Ligh, Generalized Smith's determinant, *Linear and Multilinear Algebra*, to appear.
6 P. J. McCarthy, A generalization of Smith's determinant, *Canad. Math. Bull.* 29:109–113 (1986).
7 I. Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers*, 4th ed., Wiley, New York, 1980.
8 J. J. Rotman, *The Theory of Groups: An Introduction*, Allyn and Bacon, Boston, 1973.
9 H. J. S. Smith, On the value of a certain arithmetical determinant, *Proc. London Math. Soc.* 7:208–212 (1875–76).

Received 24 March 1988; final manuscript accepted 1 September 1988