Coprimality and Divisibility in Integer Matrices

Grant Blitz
Mentor: Dr. Maxim Arnold

Oct 24-25, 2026 MIT PRIMES Conference

Relatively Prime Matrices

Let $M, N \in \mathrm{M}_n(\mathbb{Z})$. In general, matrix multiplication is not commutative. Thus we distinguish **left coprimality** from right coprimality.

Definition

Matrices M, N are left coprime if there exist $X, Y \in \mathrm{M}_n(\mathbb{Z})$ with

$$MX + NY = \mathbf{1}.$$

Relatively Prime Matrices

Let $M, N \in \mathrm{M}_n(\mathbb{Z})$. In general, matrix multiplication is not commutative. Thus we distinguish **left coprimality** from right coprimality.

Definition

Matrices M, N are left coprime if there exist $X, Y \in \mathrm{M}_n(\mathbb{Z})$ with

$$MX + NY = \mathbf{1}.$$

An analogous definition of right coprime matrices also exists, with $M, N \in \mathrm{M}_n(\mathbb{Z})$ being right coprime if there exist $X, Y \in \mathrm{M}_n(\mathbb{Z})$ with $XM + YN = \mathbf{1}$.

Relatively Prime Matrices

Let $M, N \in \mathrm{M}_n(\mathbb{Z})$. In general, matrix multiplication is not commutative. Thus we distinguish **left coprimality** from right coprimality.

Definition

Matrices M, N are left coprime if there exist $X, Y \in \mathrm{M}_n(\mathbb{Z})$ with

$$MX + NY = \mathbf{1}.$$

An analogous definition of right coprime matrices also exists, with $M, N \in \mathrm{M}_n(\mathbb{Z})$ being right coprime if there exist $X, Y \in \mathrm{M}_n(\mathbb{Z})$ with $XM + YN = \mathbf{1}$.

Remark

The condition $MX + NY = \mathbf{1}$ may be weakened to $MX + NY = C$, where C is unimodular.

Right coprimality vs left coprimality

As matrix multiplication is not commutative, one would expect left coprimality and right coprimality are different notions. Indeed, the matrices

$$M = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \qquad N = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$$

are left coprime as $M \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + N \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \mathbf{1}$, yet M and N are not right coprime, as all rows are a multiple of $(1, 1)$.

Right coprimality vs left coprimality

As matrix multiplication is not commutative, one would expect left coprimality and right coprimality are different notions. Indeed, the matrices

$$M = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \qquad N = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$$

are left coprime as $M \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + N \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \mathbf{1}$, yet M and N are not right coprime, as all rows are a multiple of $(1, 1)$.

For the rest of this talk, the notion of *"coprimality"* refers to left coprimality.

Examples of coprime matrices

Example

A unimodular matrix $M \in \mathrm{M}_n(\mathbb{Z})$ is coprime with any other matrix $N \in \mathrm{M}_n(\mathbb{Z})$, as $MM^{-1} + N0 = \mathbf{1}$.

Examples of coprime matrices

Example

A unimodular matrix $M \in \mathrm{M}_n(\mathbb{Z})$ is coprime with any other matrix $N \in \mathrm{M}_n(\mathbb{Z})$, as $MM^{-1} + N0 = \mathbf{1}$.

Example

Any matrices $M, N \in \mathrm{M}_n(\mathbb{Z})$ with coprime determinant are coprime. There exist integers a and b such that $a\det(M) + b\det(N) = 1$, so

$$M(a\,\mathrm{adj}(M)) + N(b\,\mathrm{adj}(N)) = \mathbf{1}.$$

Is the converse true?

Examples of coprime matrices

Example

A unimodular matrix $M \in \mathrm{M}_n(\mathbb{Z})$ is coprime with any other matrix $N \in \mathrm{M}_n(\mathbb{Z})$, as $MM^{-1} + N0 = \mathbf{1}$.

Example

Any matrices $M, N \in \mathrm{M}_n(\mathbb{Z})$ with coprime determinant are coprime. There exist integers a and b such that $a\det(M) + b\det(N) = 1$, so

$$M(a\,\mathrm{adj}(M)) + N(b\,\mathrm{adj}(N)) = \mathbf{1}.$$

Is the converse true? No.

Example

Let $M = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$ and $N = \begin{pmatrix} 3 & 0 \\ 0 & 4 \end{pmatrix}$. Then, $M(-\mathbf{1}) + N\mathbf{1} = \mathbf{1}$, so matrices M and N are coprime. However, $\det M = 6$ and $\det N = 12$.

A lattice interpretation of coprimality

Put the matrices M and N side by side:

$$A = \begin{pmatrix} M & N \end{pmatrix} \in \mathbb{Z}^{n \times 2n}.$$

Then, there exist $X, Y \in \mathrm{M}_n(\mathbb{Z})$ such that $MX + NY = \mathbf{1}$ if and only if $A \begin{pmatrix} X \\ Y \end{pmatrix} = \mathbf{1}$. In other words, the map $A \colon \mathbb{Z}^{2n} \to \mathbb{Z}^n$ is surjective.

A lattice interpretation of coprimality

Put the matrices M and N side by side:

$$A = \begin{pmatrix} M & N \end{pmatrix} \in \mathbb{Z}^{n \times 2n}.$$

Then, there exist $X, Y \in \mathrm{M}_n(\mathbb{Z})$ such that $MX + NY = \mathbf{1}$ if and only if $A \begin{pmatrix} X \\ Y \end{pmatrix} = \mathbf{1}$. In other words, the map $A\colon \mathbb{Z}^{2n} \to \mathbb{Z}^n$ is surjective.

Equivalent condition

The $2n$ column vectors of M and N generate the entire integer lattice $\mathbb{Z}^n$.

A coprimality theorem

Theorem

For $A \in \mathbb{Z}^{n \times 2n}$, the map $A : \mathbb{Z}^{2n} \to \mathbb{Z}^n$ is surjective exactly when

$$\boxed{\gcd\{\det(A_S) : \ S \subseteq \{1, \ldots, 2n\}, \ |S| = n\} = 1,}$$

where A_S is the $n \times n$ submatrix using columns in S.

Sketch of proof:

- If the minors have GCD 1, Bézout combinations of their determinants produce each standard basis vector.
- Otherwise some prime p divides every maximal minor, so A has rank less than n modulo p.

A modular coprimality constraint

There is a cleaner way to express our constraint on when two matrices are coprime.

Corollary

M, N are **not** coprime precisely when there are a prime p and nonzero $v \in \mathbb{F}_p^n$ such that

$$\boxed{v^{\mathsf{T}} M = v^{\mathsf{T}} N = 0 \pmod{p}.}$$

In other words, modulo some prime p, all the columns of M and N lie in some hyperplane.

Coprimality and common divisors

Over the integers, two numbers are coprime if and only if their only common factor is 1. This motivates the following question.

Coprimality and common divisors

Over the integers, two numbers are coprime if and only if their only common factor is 1. This motivates the following question.

Question

For two matrices, are they coprime if and only if every common divisor of them is unimodular?

Coprimality and common divisors

Over the integers, two numbers are coprime if and only if their only common factor is 1. This motivates the following question.

Question

For two matrices, are they coprime if and only if every common divisor of them is unimodular?

Yes, as shown by the following theorem.

Theorem

Matrices M, N are coprime if and only if every common left divisor D (so $M = DM'$, $N = DN'$) is unimodular.

Defining a matrix GCD

For integers, a greatest common divisor generates the ideal (a, b). For matrices, consider the column lattice

$$L = M\mathbb{Z}^n + N\mathbb{Z}^n \subseteq \mathbb{Z}^n.$$

Assume L has full rank, and consider its canonical Hermite normal form basis.

Definition

The matrix whose columns are this HNF basis is $\gcd(M, N)$.

This choice resolves ambiguity from multiplying a lattice basis on the right by a unimodular matrix, implying uniqueness of GCDs.

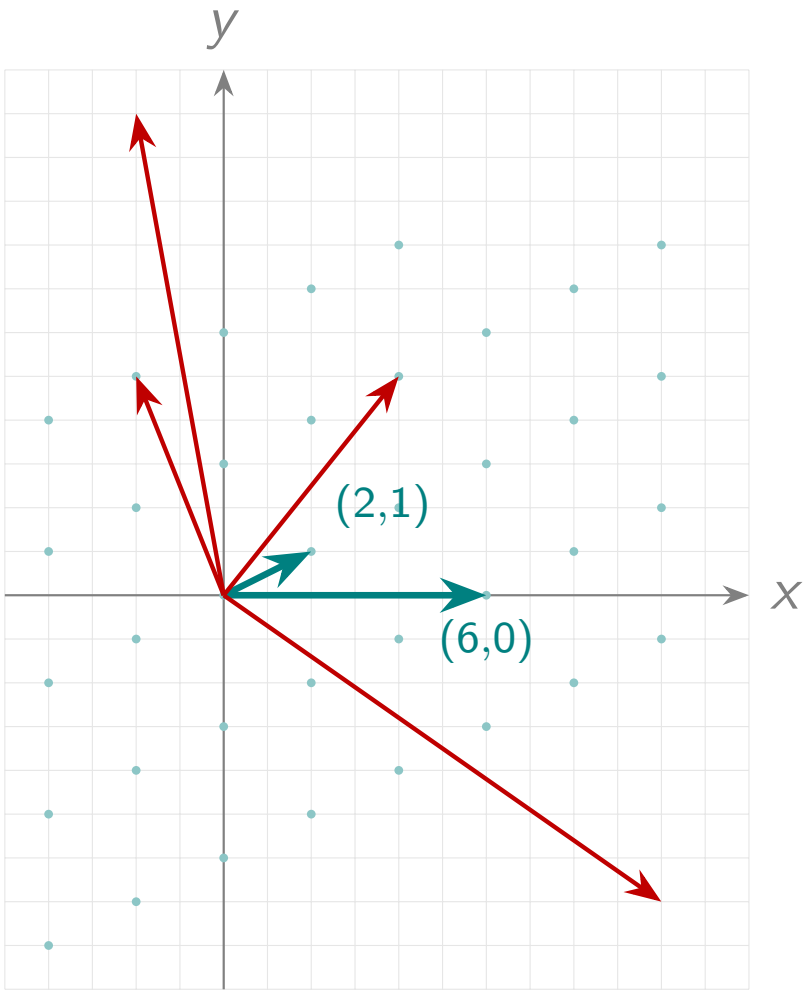
An example GCD calculation

$$M = \begin{pmatrix} 4 & -2 \\ 5 & 5 \end{pmatrix}, \quad N = \begin{pmatrix} 10 & -2 \\ -7 & 11 \end{pmatrix}.$$

The four columns generate the same lattice as

$$D = \begin{pmatrix} 6 & 2 \\ 0 & 1 \end{pmatrix}.$$

So $\gcd(M, N) = D$, as matrix D is in Hermite normal form.



Is the GCD a common divisor?

On the last slide, we established that

$$\gcd\left(\begin{pmatrix} 4 & -2 \\ 5 & 5 \end{pmatrix}, \begin{pmatrix} 10 & -2 \\ -7 & 11 \end{pmatrix}\right) = \begin{pmatrix} 6 & 2 \\ 0 & 1 \end{pmatrix}.$$

Is the GCD a common divisor?

On the last slide, we established that

$$\gcd\left(\begin{pmatrix} 4 & -2 \\ 5 & 5 \end{pmatrix}, \begin{pmatrix} 10 & -2 \\ -7 & 11 \end{pmatrix}\right) = \begin{pmatrix} 6 & 2 \\ 0 & 1 \end{pmatrix}.$$

Note we have the equalities

$$\begin{pmatrix} 4 & -2 \\ 5 & 5 \end{pmatrix} = \begin{pmatrix} 6 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & -2 \\ 5 & 5 \end{pmatrix}, \qquad \begin{pmatrix} 10 & -2 \\ -7 & 11 \end{pmatrix} = \begin{pmatrix} 6 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 4 & -4 \\ -7 & 11 \end{pmatrix}.$$

Is the GCD a common divisor?

On the last slide, we established that

$$\gcd\left(\begin{pmatrix} 4 & -2 \\ 5 & 5 \end{pmatrix}, \begin{pmatrix} 10 & -2 \\ -7 & 11 \end{pmatrix}\right) = \begin{pmatrix} 6 & 2 \\ 0 & 1 \end{pmatrix}.$$

Note we have the equalities

$$\begin{pmatrix} 4 & -2 \\ 5 & 5 \end{pmatrix} = \begin{pmatrix} 6 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & -2 \\ 5 & 5 \end{pmatrix}, \qquad \begin{pmatrix} 10 & -2 \\ -7 & 11 \end{pmatrix} = \begin{pmatrix} 6 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 4 & -4 \\ -7 & 11 \end{pmatrix}.$$

Question

Does this hold for all matrices M and N?

Some easy GCD results

Theorem

Let $M, N \in \mathbb{M}_n(\mathbb{Z})$ be integer matrices, and let $D = \gcd(M, N)$. Then, there exist matrices X and Y such that $M = DX$ and $N = DY$.

Some easy GCD results

Theorem

Let $M, N \in \mathrm{M}_n(\mathbb{Z})$ be integer matrices, and let $D = \gcd(M, N)$. Then, there exist matrices X and Y such that $M = DX$ and $N = DY$.

Theorem

Let $M, N \in \mathrm{M}_n(\mathbb{Z})$ be integer matrices. Then, there exist $X, Y \in \mathrm{M}_n(\mathbb{Z})$ such that $MX + NY = \gcd(M, N)$.

Some easy GCD results

Theorem

Let $M, N \in \mathrm{M}_n(\mathbb{Z})$ be integer matrices, and let $D = \gcd(M, N)$. Then, there exist matrices X and Y such that $M = DX$ and $N = DY$.

Theorem

Let $M, N \in \mathrm{M}_n(\mathbb{Z})$ be integer matrices. Then, there exist $X, Y \in \mathrm{M}_n(\mathbb{Z})$ such that $MX + NY = \gcd(M, N)$.

Theorem

For any three nonsingular matrices $M, N, K \in \mathrm{M}_n(\mathbb{Z})$, there exists a unimodular matrix J such that $\gcd(KM, KN) = K \gcd(M, N)J$.

What is a prime matrix?

Definition

A nonunimodular matrix $M \in \mathrm{M}_n(\mathbb{Z})$ is prime-like if, for every $N \in \mathrm{M}_n(\mathbb{Z})$, either M and N are coprime, or there exists $D \in \mathrm{M}_n(\mathbb{Z})$ such that $N = MD$.

Theorem

A matrix $M \in \mathrm{M}_n(\mathbb{Z})$ is prime-like if and only if $|\det M|$ is a prime number.

What is a prime matrix?

Definition

A nonunimodular matrix $M \in \mathrm{M}_n(\mathbb{Z})$ is prime-like if, for every $N \in \mathrm{M}_n(\mathbb{Z})$, either M and N are coprime, or there exists $D \in \mathrm{M}_n(\mathbb{Z})$ such that $N = MD$.

Theorem

A matrix $M \in \mathrm{M}_n(\mathbb{Z})$ is prime-like if and only if $|\det M|$ is a prime number.

Sketch of proof:

- If $|\det M| = p$, the column lattice has covolume p in $\mathbb{Z}^n$. Any larger lattice must precisely be $\mathbb{Z}^n$.

What is a prime matrix?

Definition

A nonunimodular matrix $M \in \mathrm{M}_n(\mathbb{Z})$ is prime-like if, for every $N \in \mathrm{M}_n(\mathbb{Z})$, either M and N are coprime, or there exists $D \in \mathrm{M}_n(\mathbb{Z})$ such that $N = MD$.

Theorem

A matrix $M \in \mathrm{M}_n(\mathbb{Z})$ is prime-like if and only if $|\det M|$ is a prime number.

Sketch of proof:

- If $|\det M| = p$, the column lattice has covolume p in $\mathbb{Z}^n$. Any larger lattice must precisely be $\mathbb{Z}^n$.
- If $|\det M|$ is composite, a prime divisor p of $|\det M|$ gives a modular constraint on the column vectors of M. This allows for the construction of $N \in \mathrm{M}_n(\mathbb{Z})$ with $|\det N| = p$ such that M is divisible by N.

Factorization exists

Theorem

Every nonunimodular integer matrix M with $\det M \neq 0$ factors as

$$\boxed{M = M_1 M_2 \cdots M_k,}$$

where each M_i is prime-like.

Sketch of proof: induction on k, the number of prime divisors of $|\det M|$, using similar techniques to the last theorem.

Acknowledgements

I would like to thank my mentor Dr. Maxim Arnold for his guidance, support, and advice throughout working on this paper. I also extend my gratitude to the MIT PRIMES program for making this research possible.

End of presentation

Thank you!