CYCLEMASTER MATRICES AND PRIMALITY TESTING

Marcin Mazur
Department of Mathematics and Statistics, Binghamton University, Binghamton, New York
mazur@math.binghamton.edu

Stephen M. Zemyan[1]
Department of Mathematics, Penn State Mont Alto, Mont Alto, Pennsylvania
smz3@psu.edu

Received: 10/25/22, Accepted: 4/6/23, Published: 4/24/23

Abstract

We define the $N \times N$ single variable cyclemaster matrix, and use its determinant to construct a necessary and sufficient test for N to be prime.

1. Introduction

We begin by defining the single variable cyclemaster matrix. At first, it may seem to be entirely irrelevant to any discussion of primality testing. However, we shall eventually see that it is actually essential in the exposition to follow. Three examples illustrate the formal definition below.

If $N = 2$, then the 2×2 single variable cyclemaster matrix is defined as

$$\mathcal{C}_2(e_1, e_2; x) = \begin{pmatrix} 1 & 1 \\ x^{e_1} & x^{e_2} \end{pmatrix}.$$

If $N = 3$, then the 3×3 single variable cyclemaster matrix is defined as

$$\mathcal{C}_3(e_1, e_2, e_3; x) = \begin{pmatrix} 1 & 1 & 1 \\ x^{e_1} & x^{e_2} & x^{e_3} \\ x^{e_1+e_2} & x^{e_2+e_3} & x^{e_3+e_1} \end{pmatrix}.$$

If $N = 4$, then the 4×4 single variable cyclemaster matrix is defined as

$$\mathcal{C}_4(e_1, e_2, e_3, e_4; x) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ x^{e_1} & x^{e_2} & x^{e_3} & x^{e_4} \\ x^{e_1+e_2} & x^{e_2+e_3} & x^{e_3+e_4} & x^{e_4+e_1} \\ x^{e_1+e_2+e_3} & x^{e_2+e_3+e_4} & x^{e_3+e_4+e_1} & x^{e_4+e_1+e_2} \end{pmatrix}.$$

DOI: 10.5281/zenodo.7859021

[1]Emeritus Professor of Mathematics

These three matrices were defined explicitly here in order to highlight the pattern evidenced by the exponents e_i in the formal definition.

Definition 1. Given a sequence $e_1, \ldots, e_N$ of real numbers, the *partial sum* m_{ij}, with $1 \leq i, j \leq N$, is the sum of j consecutive elements of our sequence starting with e_i, and is defined formally as

$$m_{ij} = e_i + \cdots + e_{i+j-1} = \sum_{k=0}^{j-1} e_{i+k},$$

with the convention that $m_{i,0} = 0$ and, when $i+k > N$, then $e_{i+k} = e_{i+k-N}$. Thus, $m_{33} = e_3 + e_4 + e_5$; but if $N = 4$, then $m_{33} = e_3 + e_4 + e_1$, as $e_5 = e_1$ in this case. Rephrased, if $i + k > N$, then the sum "wraps around" to the beginning.

The *single variable cyclemaster matrix* $\mathcal{C}_N(e_1, \ldots, e_N; x)$ is the $N \times N$ matrix whose ij^{th} entry is equal to $x^{m_{j,i-1}}$. Specifically,

$$\mathcal{C}_N(e_1, \ldots, e_N; x) = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ x^{m_{1,1}} & x^{m_{2,1}} & x^{m_{3,1}} & \cdots & x^{m_{N,1}} \\ x^{m_{1,2}} & x^{m_{2,2}} & x^{m_{3,2}} & \cdots & x^{m_{N,2}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x^{m_{1,N-1}} & x^{m_{2,N-1}} & x^{m_{3,N-1}} & \cdots & x^{m_{N,N-1}} \end{pmatrix}.$$

Matrices of this type (with $x = 2$) have previously appeared in the literature [4], where they were defined as *cyclemaster matrices*, due to their role in providing a necessary condition for the existence of N-cycles in the "$3x+1$" problem and their value as a common feature in all "$ax+1$" problems. When the sequence $e_1, \ldots, e_N$ consists of positive integers, the cyclemaster matrix is defined for any real number x; otherwise we assume that $x > 0$.

After computing the determinant of a single variable cyclemaster matrix for the first few values of N, an interesting observation was made by the second named author. If N is a prime number (2, 3, 5, 7), then the polynomial determinant vanishes identically for all x if and only if $e_1 = \cdots = e_N$. On the other hand, if N is composite (4, 6), then the polynomial determinant could vanish even if the exponents were not all equal. For example, $\det \mathcal{C}_4(e_1, e_2, e_1, e_2; x) = 0$ and $\det \mathcal{C}_6(e_1, e_2, e_3, e_1, e_2, e_3; x) = 0$ for all x. In this paper, we show that these observations remain valid for all positive integers N, thus providing a primality test.

Most primality tests are stated in terms of congruences. For example, Wilson's Theorem states that N is a prime number if and only if $(N-1)! \equiv -1 \pmod{N}$. This is a simply stated test which becomes computationally difficult for large values of N – a common characteristic of primality tests. Other tests involve the use of primitive roots, factoring $N \pm 1$, or employing sieve methods. See [1, 2] for examples. Some of the other tests for primality are probabilistic in nature in the sense that the test returns the result that N is probably a prime.

Our main result provides a characterization of prime numbers in the sense that it provides a necessary and sufficient condition for a number to be prime. Specifically, we prove the following theorem.

Theorem 1. *Let $N \geq 2$ be an integer. Then the following statements are equivalent:*

(1) *N is a prime number.*

(2) *If the determinant $\det \mathcal{C}_N(e_1, \ldots, e_N; x) = 0$ for all $x > 0$, then $e_1 = \cdots = e_N$.*

(3) *If $e_1, \ldots, e_N$ are taken from the set $\{0, 1\}$ and the determinant $\det \mathcal{C}_N(e_1, \ldots, e_N; x) = 0$ for all x, then $e_1 = \cdots = e_N$.*

Note that the primality test provided by Theorem 1 is not computationally practical due to the numerical difficulties encountered when evaluating determinants. It does not involve congruences or primitive roots and it is not probabilistic in nature. Rather, the primality of the integer N depends upon the equality of N completely unrelated parameters, and in this sense it represents a unique approach to primality testing.

We will derive Theorem 1 from the following result, which is of independent interest.

Theorem 2. *Let $c_N(e_1, \ldots, e_N; x) = \det \mathcal{C}_N(e_1, \ldots, e_N; x)$. Then $c_N(e_1, \ldots, e_N; x)$ has a zero of multiplicity at least $N - 1$ at $x = 1$ and the $(N-1)^{st}$ derivative of $c_N(e_1, \ldots, e_N; x)$ at $x = 1$ is equal to*

$$c_N^{(N-1)}(e_1, \ldots, e_N; 1) = (-1)^{\lfloor N/2 \rfloor}(N-1)! \prod_{j=1}^{N-1} \left(e_1 + e_2\omega^j + e_3\omega^{2j} + \ldots + e_N\omega^{j(N-1)} \right),$$

where ω is a primitive N^{th} root of unity.

2. Proofs of the Theorems

We start with Theorem 2. Our proof of this theorem is based on the following lemma.

Lemma 1. *Let $M(e_1, \ldots, e_N)$ denote the matrix*

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ e_1 & e_2 & \dots & e_N \\ e_1+e_2 & e_2+e_3 & \dots & e_N+e_1 \\ e_1+e_2+e_3 & e_2+e_3+e_4 & \dots & e_N+e_1+e_2 \\ \vdots & \vdots & \vdots & \vdots \\ e_1+e_2+\ldots+e_{N-1} & e_2+e_3+\ldots+e_N & \dots & e_N+e_1+\ldots+e_{N-2} \end{pmatrix}.$$

Then

$$\det M(e_1,\ldots,e_N) = (-1)^{\lfloor N/2 \rfloor} \prod_{j=1}^{N-1} \left(e_1 + e_2\omega^j + e_3\omega^{2j} + \ldots + e_N\omega^{j(N-1)} \right),$$

where ω is a primitive N^{th} root of unity.

Proof. Subtracting row $N-1$ from row N, then row $N-2$ from row $N-1$, ..., and finally row 2 from row 3, we see that

$$\det M(e_1,\ldots,e_N) = \det \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ e_1 & e_2 & e_3 & \dots & e_N \\ e_2 & e_3 & e_4 & \dots & e_1 \\ e_3 & e_4 & e_5 & \dots & e_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ e_{N-1} & e_N & e_1 & \dots & e_{N-2} \end{pmatrix}.$$

Moving the first row down to be the last and multiplying it by the sum $E = e_1 + \cdots + e_N$, we see that

$$E \cdot \det M(e_1,\ldots,e_N) = (-1)^{N-1} \det \begin{pmatrix} e_1 & e_2 & e_3 & \dots & e_N \\ e_2 & e_3 & e_4 & \dots & e_1 \\ e_3 & e_4 & e_5 & \dots & e_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ e_{N-1} & e_N & e_1 & \dots & e_{N-2} \\ E & E & E & \dots & E \end{pmatrix}.$$

Subtracting from the last row the sum of all the other rows, we get that

$$E \cdot \det M(e_1,\ldots,e_N) = (-1)^{N-1} \det \begin{pmatrix} e_1 & e_2 & e_3 & \dots & e_N \\ e_2 & e_3 & e_4 & \dots & e_1 \\ e_3 & e_4 & e_5 & \dots & e_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ e_{N-1} & e_N & e_1 & \dots & e_{N-2} \\ e_N & e_1 & e_2 & \dots & e_{N-1} \end{pmatrix}.$$

Permuting the rows according to the permutation $\begin{pmatrix} 1 & 2 & 3 & \dots & N \\ 1 & N & N-1 & \dots & 2 \end{pmatrix}$, which is a product of $\lfloor (N-1)/2 \rfloor$ transpositions, we get that

$$E \cdot \det M(e_1, \dots, e_N) = (-1)^{N-1}(-1)^{\lfloor (N-1)/2 \rfloor} \det \begin{pmatrix} e_1 & e_2 & e_3 & \dots & e_N \\ e_N & e_1 & e_2 & \dots & e_{N-1} \\ e_{N-1} & e_N & e_1 & \dots & e_{N-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ e_3 & e_4 & e_5 & \dots & e_2 \\ e_2 & e_3 & e_4 & \dots & e_1 \end{pmatrix}.$$

The matrix on the right is the *circulant matrix*. Its determinant is given by the following formula [3, page 75]:

$$E \prod_{j=1}^{N-1} \left(e_1 + e_2\omega^j + e_3\omega^{2j} + \ldots + e_N\omega^{j(N-1)} \right).$$

This easily implies the assertion of Lemma 1 when $E \neq 0$. The case $E = 0$ follows by a straightforward continuity argument. □

Proof of Theorem 2. Subtracting the first row of $\mathcal{C}_N(e_1, \dots, e_N; x)$ from each of the other rows and then dividing each row except the first one by $(x-1)$ we see that

$$\frac{c_N(e_1, \dots, e_N; x)}{(x-1)^{N-1}}$$
$$= \det \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ \frac{x^{e_1}-1}{x-1} & \frac{x^{e_2}-1}{x-1} & \frac{x^{e_3}-1}{x-1} & \dots & \frac{x^{e_N}-1}{x-1} \\ \frac{x^{e_1+e_2}-1}{x-1} & \frac{x^{e_2+e_3}-1}{x-1} & \frac{x^{e_3+e_4}-1}{x-1} & \dots & \frac{x^{e_N+e_1}-1}{x-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \frac{x^{e_1+e_2+\ldots+e_{N-1}}-1}{x-1} & \frac{x^{e_2+e_3+\ldots+e_N}-1}{x-1} & \frac{x^{e_3+\ldots+e_N+e_1}-1}{x-1} & \dots & \frac{x^{e_N+e_1+\ldots+e_{N-2}}-1}{x-1} \end{pmatrix}.$$

Recall that for any real number k we have $\lim_{x\to 1}(x^k - 1)/(x-1) = k$. It follows that when x tends to 1, the matrix on the right side converges to the matrix $M(e_1, \dots, e_N)$. Thus

$$\lim_{x\to 1} \frac{c_N(e_1, \dots, e_N; x)}{(x-1)^{N-1}} = \det M(e_1, \dots, e_N).$$

Recall now a simple result from calculus: if $R(x)$ is a function of class C^k and $\lim_{x\to 1} \frac{R(x)}{(x-1)^k} = L$ exists then $R^{(i)}(1) = 0$ for $i < k$ and $R^{(k)}(1) = k!L$. Applying this to $R(x) = c_N(e_1, \dots, e_N; x)$ and $k = N-1$ we see that $c_N^{(i)}(e_1, \dots, e_N; 1) = 0$ for $0 \leq i < N-1$ and

$$c_N^{(N-1)}(e_1, \dots, e_N; 1) = (N-1)! \det M(e_1, \dots, e_N).$$

Theorem 2 follows now from Lemma 1. □

For our proof of Theorem 1 we need the following simple lemma.

Lemma 2. *If $u_1 < \ldots < u_n$ and $a_1, \ldots, a_n$ are real numbers such that $\sum_{k=1}^{n} a_k x^{u_k} = 0$ for all $x > 0$, then $a_k = 0$ for all k.*

Proof. We use induction on n. The case $n = 1$ is clear. Assume that $n > 1$ and the result holds for $n-1$. By taking the derivative with respect to x and then multiplying by x we get $\sum_{k=1}^{n} a_k u_k x^{u_k} = 0$. It follows that $\sum_{k=1}^{n-1} a_k(u_k - u_n)x^{u_k} = 0$. By the inductive assumption we conclude that $a_k = 0$ for $k = 1, \ldots, n-1$. This also forces $a_n = 0$. □

We will use the following straightforward consequence of Lemma 2.

Corollary 1. *If $\sum_{i=1}^{K} x^{k_i} = \sum_{i=1}^{M} x^{m_i}$ for all $x > 0$ and some (not necessarily distinct) real numbers $k_1, \ldots, k_K$ and $m_1, \ldots, m_M$, then $K = M$ and there is a permutation f of $1, 2, \ldots, K$ such that $k_i = m_{f(i)}$ for $i = 1, \ldots, K$.*

Proof of Theorem 1. Note that for any integer $N > 1$, if $e_1 = \cdots = e_N$, then $\det \mathcal{C}_N(e_1, \ldots, e_N; x) = 0$ for all x, since the second row of $\mathcal{C}_N(e_1, \ldots, e_N; x)$ is a multiple of the first row.

It is obvious that (2) implies (3).

If N is composite and $D > 1$ is a proper divisor of N then $\det \mathcal{C}_N(e_1, \ldots, e_N; x)$ vanishes as a function of x for any sequence $e_1, \ldots, e_N$ which has period D (i.e. $e_{i+D} = e_i$ for all i). Indeed, in this case the $(D+1)^{st}$ row of the matrix $\mathcal{C}_N(e_1, \ldots, e_D, e_{D+1}, \ldots, e_N; x)$ is a scalar multiple of the first row, since every entry in the $(D+1)^{st}$ row is equal to x^{S_D}, where $S_D = e_1 + \cdots + e_D$. This, in particular, shows that statement (3) implies statement (1).

It remains to prove that (1) implies (2), which is the hard part of our result. We proceed by contradiction. Assume that N is prime and $c_N(e_1, \ldots, e_N; x) = 0$ for all $x > 0$ and some non-constant sequence $e_1, \ldots, e_N$ of real numbers. Using the Leibniz formula for the determinant $\det \mathcal{C}_N(e_1, \ldots, e_N; x)$ we see that

$$\sum_{\sigma \in S_N} (-1)^{\mathrm{sign}(\sigma)} x^{L_\sigma(e_1, \ldots, e_N)} = 0,$$

where S_N is the set of all permutations of $\{1, 2, \ldots, N\}$ and each L_σ is a linear homogeneous form in $e_1, \ldots, e_N$ with integer coefficients. In other words,

$$\sum_{\sigma odd} x^{L_\sigma(e_1, \ldots, e_N)} = \sum_{\sigma even} x^{L_\sigma(e_1, \ldots, e_N)}.$$

Corollary 1 implies that there is a bijection f from odd permutations to even permutations such that $L_\sigma(e_1, \ldots, e_N) = L_{f(\sigma)}(e_1, \ldots, e_N)$ for every odd permutation σ. We can view the equalities $L_\sigma(e_1, \ldots, e_N) = L_{f(\sigma)}(e_1, \ldots, e_N)$ as a system of homogeneous linear equations in $e_1, \ldots, e_N$ with integer coefficients which

has a non-constant real solution. But then it also has a non-constant integral solution. Thus there is a non-constant sequence $e'_1, \ldots, e'_N$ of integers such that $c_n(e'_1, \ldots, e'_N; x) = 0$ for all $x > 0$. By Theorem 2, we have

$$\prod_{j=1}^{N-1} \left(e'_1 + e'_2\omega^j + e'_3\omega^{2j} + \ldots + e'_N\omega^{j(N-1)} \right) = 0,$$

where ω is a primitive N-th root of unity. Thus one of the factors in the product must be 0. Now since N is a prime, ω^j is also a primitive N^{th} root of unity for $1 \leq j < N$. Thus we have $e'_1 + e'_2\tau + \ldots + e'_N\tau^{N-1} = 0$ for a primitive N^{th} root of unity τ. Note that $1 + \tau + \ldots + \tau^{N-1} = 0$, so we have $(e'_1 - e'_N) + (e'_2 - e'_N)\tau + \ldots + (e'_{N-1} - e'_N)\tau^{N-2} = 0$. Moreover, $1 + x + \ldots + x^{N-1}$ is the minimal polynomial for τ, so $e'_i - e'_N = 0$ for $i = 1, \ldots, N-1$. In other words, $e'_1 = \ldots = e'_N$, a contradiction. □

References

[1] A. Granville, It is easy to determine whether a given integer is prime, *Bull. Amer. Math. Soc.* **42** (2005), 3-38.

[2] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective*, second edition, Springer, New York, 2005.

[3] P. J. Davis, *Circulant Matrices*, AMS Chelsea Publishing, Providence, Rhode Island, 1979.

[4] S. M. Zemyan, Cyclemaster matrices and Collatz cycles, *Integers* **20** (2020), #A82, 42 pp.