Fermat's Little Theorem for Matrices and Königsberg Pseudoprimes

Aditya Gupta, Diana Harambaș, Zejia He, Aleksa Sotirov
Counsellor: Dragoș Crișan

August 2022

Abstract

In this paper, we study an extension of Fermat's Little Theorem to matrices and the pseudoprimes generated by this primality test. First, we provide two proofs of Fermat's Little Theorem for matrices. We then consider the infinitude of pseudoprimes for various classes of matrices and also investigate so-called 'PROMYS pseudoprimes', an extension of Carmichael numbers. We finish by presenting numerical data and stating our unproved conjectures.

Contents

1 Introduction

This paper explores Fermat's Little Theorem for matrices and pseudoprimes generated by Fermat's Primality Test for matrices. In Section 2, we introduce Fermat's Little Theorem and Fermat Primality Test for both integers and matrices. We also provide an introduction to linear algebra ideas, which will be utilized in later sections. In Section 3, we proceed to present two proofs of Fermat's Little Theorem using number theory and group theory respectively. In Section 4, we consider infinite families of pseudoprimes by studying 2×2, 3×3, and $n \times n$ matrices and provide proofs for our conjectures. We also investigate 'PROMYS pseudoprimes' by providing a generalization of Carmichael numbers. In Section 5, we present some observations of pseudoprimes and a series of unproved conjectures that may be of interest for further exploration. We also show a graph displaying the frequency of appearance of pseudoprimes in the Königsberg matrix.

2 Fermat's Little Theorem

2.1 Fermat's Little Theorem for integers

First, we will provide some background on this topic by defining and explaining concepts including Fermat's Little Theorem (FℓT), the Fermat Primality Test and pseudoprimes.

Theorem 2.1 (FℓT)**.** *Let p be a prime number. Then for any integer a, we have that*

$$a^p \equiv a \ (mod\ p).$$

This is the version of (FℓT) that we will use in this paper.

Fermat Primality Test. *If there exists an integer a such that $a^n \not\equiv a \ (mod\ n)$, then n is not prime.*

The Fermat Primality Test is rather a *compositeness* test that checks if numbers are composite. For example,

$$2^{12} \equiv 4 \ (\text{mod } 12),$$

and so 12 is not prime. Since using base 2 shows that 12 is not prime, we call 2 a **Fermat witness** for 12.

Fermat Pseudoprimes. Although the Fermat Primality Test is mostly

correct, it occasionally lets composite numbers slip through. Any composite number n for which there exists an integer a such that $a^n \equiv a \pmod{n}$ is called a **Fermat pseudoprime**. For example,

$$3^{91} \equiv 3 \pmod{91},$$

despite the fact that $91 = 13 \cdot 7$ is composite. So, we say that 91 is a **base 3 pseudoprime**.

Pseudoprimes in a particular base are relatively rare. The probability of a base 3 pseudoprime occurring for a number $n \leq 10^9$ is about one in ten thousand, while the probability of a prime occurring up to 10^9 is about one in twenty.

It is also often possible to retest a number with a different base. For example,

$$2^{91} \equiv 37 \pmod{91},$$

showing that 91 is composite.

However, there are numbers that are pseudoprimes in *every base*. They are called **Carmichael numbers**, with the smallest example being $561 = 3 \cdot 11 \cdot 13$. We present an important result about Carmichael numbers:

Korselt's Criterion: A composite integer n divides $a^n - a$ for all integers a if and only if n is squarefree and $n \equiv 1 \pmod{p-1}$ for all prime divisors p of n.

2.2 Fermat's Little Theorem for matrices

In order to expand FℓT to matrices, we will introduce some linear algebra. In this paper, we consider only square matrices, that is, $n \times n$ matrices.

Let M be an $n \times n$ matrix with entries $(a_{i,j})$ in a field K, where i is the row number and j is the column number.

$$M = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{pmatrix}$$

Trace of a square matrix.

The **trace** of a square matrix is the sum of the elements along the diagonal from top left to bottom right, i.e.

$$\mathrm{Tr}(M) = a_{1,1} + a_{2,2} + ... + a_{n,n} = \sum_{i=1}^{n} a_{i,i}$$

Moreover, $n \times n$ matrices form a ring $\mathcal{M}_n$ under addition and multiplication. As in any ring there is a multiplicative identity; here we have the **identity matrix** I such that for any matrix M, $M \cdot I = I \cdot M = M$, with I being:

$$I = \begin{pmatrix} 1 & 0 & ... & 0 \\ 0 & 1 & ... & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & ... & 1 \end{pmatrix}$$

The determinant of a matrix.

For $n \times n$ matrices, we define the determinant as

$$\det(M) := \sum_{\tau \in S_n} (\mathrm{sgn}(\tau) \prod_{i=1}^{n} a_{i,\tau_i}),$$

where the sum is over all τ permutations of $\{1, 2, ..., n\}$.

For 2x2 matrices, the determinant is:

$$\det(M) = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

For 3x3 matrices, it is:

$$\det(M) = \det \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = aei + cdh + bfg - ceg - bdi - ahf$$

If $\det(M) \neq 0$, then matrix M is **invertible**.

The characteristic polynomial of a matrix.

For an $n \times n$ matrix M, this is an n-degree polynomial $\chi_M(x) = \det(M - x \cdot I)$.

Its n roots are called the eigenvalues of the matrix, conventionally written as $\lambda_1, \lambda_2, ..., \lambda_n$.

Remark: If the matrix has integral entries, then all coefficients of the characteristic polynomial are integers.

Properties of eigenvalues.

$$\mathrm{Tr}(M) = \lambda_1 + \lambda_2 + ... + \lambda_n$$

$$\det(M) = \lambda_1 \cdot \lambda_2 \cdot ... \cdot \lambda_n$$

After **matrix exponentiation**, for any natural number k, the matrix M^k will have the eigenvalues $\lambda_1^k, \lambda_2^k, ..., \lambda_n^k$.

As λ_i is a root of χ we have $\chi(\lambda_i) = 0$, so $\lambda_i^{m-n} \cdot \chi(\lambda_i) = 0$, for $m \geq n$. This gives a recurrence relation for λ_i^m in terms of the lower powers of λ_i.

For example, take the degree three polynomial $\chi(x) = x^3 - 5x^2 - 17x + 21$. This factorises into $\chi(x) = (x-7)(x-1)(x+3)$, so the eigenvalues are $\lambda_1 = 7, \lambda_2 = 1, \lambda_3 = -3$.

The trace of the corresponding matrices is $\mathrm{Tr}(M) = \lambda_1 + \lambda_2 + \lambda_3 = 5$, respecting Vieta's formulae, alongside with the other coefficients $\lambda_1\lambda_2 + \lambda_2\lambda_3 + \lambda_3\lambda_1 = -17$ and $\det(M) = \lambda_1\lambda_2\lambda_3 = -21$.

We can thus find a recurrence relation: $\chi(\lambda_i) = \lambda_i^3 - 5\lambda_i^2 - 17\lambda_i + 21 = 0$ gives us $\lambda_i^3 = 5\lambda_i^2 + 17\lambda_i - 21$ and, further, by multiplying all terms with λ_i^{n-3} we get: $\lambda_i^n = 5\lambda_i^{n-1} + 17\lambda_i^{n-2} + 21\lambda_i^{n-3}$, for any $i \in \{1, 2, 3\}$.

Symmetric matrices.

Let M be an $n \times n$ matrix with entries $(a_{i,j})$. Then M is called **symmetric** if and only if $a_{i,j} = a_{j,i}$ for any i, j.

One of the most important properties of symmetric matrices is that a square symmetric matrix M is **diagonalizable**, i.e. there is an invertible matrix P and a diagonal matrix D such that

$$M = P \cdot D \cdot P^{-1} \text{ and } D = \begin{pmatrix} \lambda_1 & 0 & ... & 0 \\ 0 & \lambda_2 & ... & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & ... & \lambda_n \end{pmatrix},$$

where $\lambda_1, \lambda_2, ..., \lambda_n$ are the eigenvalues of M.

Moreover, for any natural k

$$M^k = P \cdot \begin{pmatrix} \lambda_1^k & 0 & ... & 0 \\ 0 & \lambda_2^k & ... & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & ... & \lambda_n^k \end{pmatrix} \cdot P^{-1}$$

Block diagonal matrices.

Let $M, M_1, M_2, ..., M_k$ be square matrices. M is a **block diagonal matrix** if it can be written as:

$$M = \begin{pmatrix} M_1 & 0 & ... & 0 \\ 0 & M_2 & ... & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & ... & M_k \end{pmatrix}.$$

For example, let the 2x2 matrices $M_1 = I_2$ and $M_2 = 5 \cdot I_2$. The block diagonal matrix M will be:

$$M = \begin{pmatrix} \mathbf{1} & \mathbf{0} & 0 & 0 \\ \mathbf{0} & \mathbf{1} & 0 & 0 \\ 0 & 0 & \mathbf{5} & \mathbf{0} \\ 0 & 0 & \mathbf{0} & \mathbf{5} \end{pmatrix}.$$

Remark: The eigenvalues of the block matrix M include all the eigenvalues of each $M_1, M_2, ..., M_k$. Moreover,

$$\mathrm{Tr}(M) = \mathrm{Tr}(M_1) + \mathrm{Tr}(M_2) + ... + \mathrm{Tr}(M_k)$$
$$\det(M) = \det(M_1) \cdot \det(M_2) \cdot ... \cdot \det(M_k)$$

Just as exponentiation works for symmetric matrices in the diagonalised form, we have that for the block diagonal matrix M:

$$M^n = \begin{pmatrix} M_1^n & 0 & ... & 0 \\ 0 & M_2^n & ... & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & ... & M_k^n \end{pmatrix}$$

We can now state FℓT for matrices.

Theorem 2.2 (FℓT for matrices)**.** *Let p be a prime number and let M be a square $n \times n$ matrix consisting of integers. Then*

$$Tr(M^p) \equiv Tr(M) \ (mod\, p)$$

This theorem can be used to give a generalised version of primality tests using matrices.

Fermat Primality Test for Matrices. For any square matrix of integers M, if $\mathrm{Tr}(M^n) \not\equiv \mathrm{Tr}(M) \pmod{n}$, then n is composite.

Like the test for integers, composite numbers that pass the Fermat Primality Test are called **pseudoprimes**, or more specifically, **matrix M Fermat pseudoprimes**.

3 Proving FℓT for matrices

In this section, we will lay out two proofs of FℓT for matrices - one completely in the spirit of number theory, and one based on concepts from group theory.

We will start with the number theory proof, in which one of the key steps will be the Fundamental Theorem of Symmetric Polynomials, known also as Newton's Theorem.

Symmetric polynomial in n variables.

Let A be a commutative ring and let $A[X_1, X_2, ..., X_n]$ be the ring of polynomials with n indeterminates over it. Let $P(x_1, x_2, ..., x_n)$ be a polynomial in $A[X_1, X_2, ..., X_n]$. P is called **symmetric** if and only if, for all permutations $x_{\tau(1)}, x_{\tau(2)}, ..., x_{\tau(n)}$ of $x_1, x_2, ..., x_n$ we have

$$P(x_1, x_2, ..., x_n) = P(x_{\tau(1)}, x_{\tau(2)}, ..., x_{\tau(n)}).$$

We define $\sigma_1, \sigma_2, ..., \sigma_n$ as follows:

$$\sigma_1 = x_1 + x_2 + ... + x_n$$

$$\vdots$$

$$\sigma_i = \sum_{\tau(1)<\tau(2)<...<\tau(i)} \left(x_{\tau(1)} x_{\tau(2)} ... x_{\tau(i)}\right)$$

$$\vdots$$

$$\sigma_n = x_1 x_2 ... x_n$$

Using this notation, we can state **The Fundamental Theorem of Symmetric Polynomials**:

Theorem 3.1. *Any symmetric polynomial P in the n-variable polynomial ring $A[X_1, X_2, ..., X_n]$ has a unique representation as a polynomial Q in the n-variable polynomial ring $A[\sigma_1, \sigma_2, ..., \sigma_n]$.*

3.1 FℓT proof by Number Theory

We can now use this theorem for our proof. To gain some intuition for our proof we will first present the specific case of 2×2 matrices.

Proof. (2×2 case)

Let λ_1, λ_2 be the eigenvalues of M. From Vieta's formulae:

$$\sigma_1 = \mathrm{Tr}(M) = \lambda_1 + \lambda_2$$

$$\sigma_2 = \det(M) = \lambda_1 \lambda_2.$$

From the properties of matrix exponentiation, we know that the eigenvalues of M^p are λ_1^p and λ_2^p and thus the trace is $\mathrm{Tr}(M^p) = \lambda_1^p + \lambda_2^p$.

We are required to prove that

$$\lambda_1^p + \lambda_2^p \equiv \lambda_1 + \lambda_2 \pmod{p}.$$

In general, the eigenvalues are not integers, so we cannot simply apply the already known version of Fermat's Little Theorem. We will have to consider the binomial expansion of $(\mathrm{Tr}(M))^p = (\lambda_1 + \lambda_2)^p$.

$$\begin{aligned}
(\mathrm{Tr}(M))^p = (\lambda_1 + \lambda_2)^p &= \sum_{k=0}^{p} \binom{p}{k} \lambda_1^{p-k} \lambda_2^k \\
&= \lambda_1^p + \lambda_2^p + \sum_{k=1}^{p-1} \binom{p}{k} \lambda_1^{p-k} \lambda_2^k \\
&= \mathrm{Tr}(M^p) + \sum_{k=1}^{\frac{p-1}{2}} \binom{p}{k} (\lambda_1^{p-k} \lambda_2^k + \lambda_1^k \lambda_2^{p-k}) \\
&= \mathrm{Tr}(M^p) + \sum_{k=1}^{\frac{p-1}{2}} \binom{p}{k} \lambda_1^k \lambda_2^k \cdot (\lambda_1^{p-2k} + \lambda_2^{p-2k})
\end{aligned}$$

$$= \mathrm{Tr}(M^p) + \sum_{k=1}^{\frac{p-1}{2}} \binom{p}{k} \det(M^k) \cdot \mathrm{Tr}(M^{p-2k})$$
$$\equiv \mathrm{Tr}(M^p) \pmod{p}$$

We know that each $\binom{p}{k}$ is divisible by p because every binomial coefficient is divisible by p. Also, each $\det(M^k)$ and $\mathrm{Tr}(M^{p-2k})$ is an integer since they are coefficients in the characteristic polynomials of matrices M^k, M^{p-2k}, which have integer entries.

Since $\mathrm{Tr}(M)$ is an integer, by Fermat's Little Theorem, the following holds:

$$(\mathrm{Tr}(M))^p \equiv \mathrm{Tr}(M) \pmod{p}.$$

So, from these two relations:

$$(\mathrm{Tr}(M))^p \equiv \mathrm{Tr}(M^p) \equiv \mathrm{Tr}(M) \pmod{p},$$

and FℓT for 2×2 matrices is proved. □

Now that we have a sense of what is happening in 2x2 matrices, we can present the proof for the general case.

Proof. (General $n \times n$ case)

This time, the roots of the characteristic polynomial (the eigenvalues) are $\lambda_1, \lambda_2, ..., \lambda_n$ and the trace is $\mathrm{Tr}(M) = \sigma_1 = \lambda_1 + \lambda_2 + ... + \lambda_n$.

In order to prove Fermat's Little Theorem, one must show that

$$\mathrm{Tr}(M^p) = \lambda_1^p + \lambda_2^p + ... + \lambda_n^p \equiv \lambda_1 + \lambda_2 + ... + \lambda_n \pmod{p}.$$

Consider the expansion of

$$(\mathrm{Tr}(M))^p = (\lambda_1 + \lambda_2 + ... + \lambda_n)^p =$$
$$= \lambda_1^p + \lambda_2^p + ... + \lambda_n^p + \alpha =$$
$$= \mathrm{Tr}(M^p) + \alpha,$$

where α is the sum of all the other terms that appear in the expansion.

Let $S(i_1, i_2, ..., i_n)$, with $0 \leq i_1 \leq i_2 \leq ... \leq i_n \leq p-1$, and $i_1+i_2+...+i_n = p$ be:

$$S(i_1, i_2, ..., i_n) = \sum_{\tau} \lambda_{\tau(1)}^{i_1} \cdot \lambda_{\tau(2)}^{i_2} \cdot ... \cdot \lambda_{\tau(n)}^{i_n},$$

where the sum is over all permutations of the eigenvalues.

Every S will be a symmetric polynomial in n-variables (the eigenvalues raised symmetrically to certain powers) and it will be followed by an n-nomial expansion coefficient $\binom{p}{i_1,i_2,...,i_n,}$ which is divisible by p. So,

$$\alpha = \sum \binom{p}{i_1, i_2, ..., i_n} S(i_1, i_2, ..., i_n),$$

where $0 \leq i_1 \leq i_2 \leq ... \leq i_n \leq p-1$, and $i_1 + i_2 + ... + i_n = p$. But as S is a symmetric polynomial, from Theorem 3.1, we get that every S has a unique polynomial representation in the commutative ring $\mathbb{Z}[\sigma_1, \sigma_2, ..., \sigma_n]$, with all σ_j integers. This means that every S actually has an integer value.

Hence, all expansion coefficients, which are multiples of p, are grouped with integers S, making each term from the sum in α be divisible by p.

$$p| \left(\binom{p}{i_1, i_2, ..., i_n} S(i_1, i_2, ..., i_n) \right)$$

Thus, $(\mathrm{Tr}(M))^p \equiv \mathrm{Tr}(M^p) \pmod{p}$. And, as the trace is an integer, applying FℓT on integers: $(\mathrm{Tr}(M))^p \equiv \mathrm{Tr}(M) \pmod{p}$.

Therefore, $\mathrm{Tr}(M^p) \equiv \mathrm{Tr}(M) \pmod{p}$, proving Fermat's Little Theorem for $n \times n$ matrices. □

3.2 FℓT proof by Group Theory

We will now lay out a proof via group theory, which requires more background. (Note that this proof only works for symmetric matrices.) Let us first state a few important facts about actions of groups that will be of use in our proof:

Theorem 3.2 (Orbit-Stabiliser Theorem)**.** *Let a finite group G act on a finite set X, and fix an element $x \in X$. Let Gx denote the orbit of x, and $Stab_G(x)$ the stabiliser of x. Then:*

$$|G| = |Gx| \cdot |Stab_G(x)|$$

Theorem 3.3 (Fixed point theorem for p-groups)**.** *Let G be a finite group of order p^n, where p is prime and $n \in \mathbb{N}$. Let G act on a finite set X, and let X^G denote the set of fixed points of X under G, i.e. $X_G = \{x \in X \mid (\forall g \in G)\, gx = x\}$. Then:*

$$|X^G| \equiv |X| \ (mod\, p)$$

We will now introduce the concept of a graph's **adjacency matrix**. Namely, if we take any graph Γ, with vertices numbered 1 to n, then we can represent it using an $n \times n$ matrix by simply filling position (i, j) in the matrix with the number of edges from vertex i to vertex j. Notice that an edge from i to j is the same as an edge from j to i, so an adjacency matrix is by necessity symmetric. We can now prove a lemma pertaining to adjacency matrices:

Lemma 3.4. *If M is the adjacency matrix of graph Γ, and k is a natural number, then position (i, j) in the matrix M^k corresponds to the number of paths from i to j in the graph Γ of length k.*

Proof. We will prove this by induction on k.

The base case, $k = 1$, holds by the definition of an adjacency matrix.

Now, let:

$$M^k = \begin{pmatrix} a_{1,1}^{(k)} & a_{1,2}^{(k)} & \dots & a_{1,m}^{(k)} \\ a_{2,1}^{(k)} & a_{2,2}^{(k)} & \dots & a_{2,m}^{(k)} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1}^{(k)} & a_{m,2}^{(k)} & \dots & a_{m,m}^{(k)} \end{pmatrix}$$

Assume that $a_{i,j}^{(k)}$ denotes the number of length n paths from i to j. Then, $M^{k+1} = M^k \cdot M$, so by definition of matrix multiplication we get:

$$a_{i,j}^{(k+1)} = \sum_{l=1}^{m} a_{i,l}^{(k)} \cdot a_{l,j}^{(1)}$$

By the induction hypothesis, $a_{i,l}^{(k)}$ is the number of length n paths from i to l, whereas $a_{l,j}^{(1)}$ is the number of single steps from l to j. This is the number of paths from i to j with penultimate vertex l, so summing up for all l simply gives us all the $(k+1)$-length paths from i to j.

□

Finally, let's prove Fermat's Little Theorem for matrices:

Proof. In order to apply these theorems, we will need to define a useful group action. Fix prime p and matrix M, and let $G = \mathbb{Z}_p$. Now, let X be the set of all round-trip p-length walks on the graph whose adjacency matrix is M. Now G can act on X by cyclically shifting the walk, e.g. the element 2 would shift the walk $2 \to 5 \to 3 \to 4 \to 1 \to 2$ to $3 \to 4 \to 1 \to 2 \to 5 \to 3$. Now, by the fixed point theorem:

$$|X^G| \equiv |X| \pmod{p}$$

Fixed points in X are walks which do not change under such rotations, which means that they must consist of only the same edge repeating. Since they must be round-trip walks as well, this means that they are sequences of p loops around the same vertex. Note that a loop on the graph corresponds to a_{ii} on the matrix, so in other words the number of such loops is exactly $\mathrm{Tr}(M) = |X^G|$.

On the other hand, by Lemma 3.4, we know that the number of p-length round trip walks on this graph is precisely $\mathrm{Tr}(M^p) = |X|$. Now, by the fixed point theorem, we have:

$$\mathrm{Tr}(M) \equiv \mathrm{Tr}(M^p) \pmod{p}$$

An adjacency matrix, by necessity, has non-negative elements. To extend the proof to matrices with negative elements, we know that adding arbitrary multiples of p does not change anything modulo p, so we can shift the entire matrix up by a multiple of p and apply this proof to the new matrix with positive integer coefficients. □

4 Infinite families of pseudoprimes

The second part of our project is concerned with the search for pseudoprimes to a specific matrix base. Our motivating question was whether all matrices have infinitely many pseudoprimes. While we did not answer this question in full generality, we made substantial progress when considering matrices with traces equal to 0 and ± 1.

We introduce the following notation. Consider a polynomial ring $\mathbb{Z}[X_1, \cdots, X_n]$. We define S, a function from $\mathbb{Z}^n$ to this ring, as follows:

$$S(m_1, m_2, \cdots, m_n) = \sum_{\tau} \left(\prod_{i=1}^{n} {X_{\tau(i)}}^{m_i} \right)$$

The sum is taken over all permutations τ of the n indeterminates $X_1, X_2, \cdots, X_n$. Each m_i is some fixed non-negative integer. We will additionally usually have $m_1 \geq m_2 \cdots \geq m_n$. If $m_i = 0$, it is omitted from the inputs to the function. Often the variables u, v, w are used in place of X_1, X_2, X_3. For example:

$$S(3,2,1) = u^3v^2w + u^3vw^2 + u^2v^3w + u^2vw^3 + uv^3w^2 + uv^2w^3$$

$$S(2,1) = u^2v + u^2w + v^2u + v^2w + w^2u + w^2v$$

Additionally, let $K(n)$ denote the sum of the nth powers of the eigenvalues of our matrix, i.e. the trace of our matrix raised to the power n. Let $\rho(\sigma_i, k)$ be the sum of the raising of each term of an elementary symmetrical polynomial to a power k, as so:

$$\rho(\sigma_2[u,v,w], 2) = (uv)^2 + (vw)^2 + (wu)^2$$

4.1 2×2 case study

We first consider matrices of the form $M = \begin{pmatrix} 1 & a \\ a & 0 \end{pmatrix}$.

Theorem 4.1. *If p is a prime and $p|a$, then all powers of p are M-pseudoprimes.*

Proof. The characteristic polynomial of M is $\chi_M(x) = x^2 - x - a^2$ and the eigenvalues λ_1, λ_2 satisfy the following:

$$\lambda_1 + \lambda_2 = 1$$
$$\lambda_1\lambda_2 = -a^2$$

The conditions of the statement give us that $p|a \Rightarrow p| - a^2$, so let $-a^2 = pk$ for $k \in \mathbb{Z}$.

Then we have p^n, with $n \in \mathbb{N}$, is an M-pseudoprime if and only if:

$$\mathrm{Tr}(M^{p^n}) \equiv \mathrm{Tr}(M) \pmod{p^n}$$
$$\Leftrightarrow \ {\lambda_1}^{p^n} + {\lambda_2}^{p^n} \equiv 1 \pmod{p^n}$$

We will prove that this identity holds for all $n \geq 0$ using induction. The base case for $n = 0$ is true since:

$${\lambda_1}^{p^0} + {\lambda_2}^{p^0} = \lambda_1 + \lambda_2 = 1 \equiv 1 \pmod{p^n}$$

Suppose the statement is true for n. We have to show this implies that it is also true for $n + 1$.

Let $u = {\lambda_1}^{p^n}, v = {\lambda_2}^{p^n}$. We know $u + v \equiv 1 \pmod{p^n}$, and we want to show that $u^p + v^p \equiv 1 \pmod{p^{n+1}}$. From the binomial expansion, we can write $(u+v)^p = u^p + v^p + uv \cdot \alpha$, where α makes up the rest of the terms of the expansion. From the expansion and from the induction step, we know that $(u+v)^p \equiv 1 \pmod{p^{n+1}}$, and $uv = (-a^2)^{p^n} = (p \cdot k)^{p^n} = p^{n+1} \cdot p^{p^n - n - 1} \cdot k^{p^n}$ is divisible by p^{n+1}.

Thus $u^p + v^p = (u+v)^p - u \cdot v \cdot \alpha \equiv 1 \pmod{p^{n+1}}$, and so the statement is true for $n+1$. By the principle of mathematical induction, we obtain that p^n is an M-pseudoprime, for all natural n. □

4.2 3×3 matrices with trace 0

Consider matrices with the characteristic polynomial of the form

$$\chi_M(x) = x^3 + bx + c$$

An example of such a matrix is $M = \begin{pmatrix} 0 & 0 & -c \\ 1 & 0 & -b \\ 0 & 1 & 0 \end{pmatrix}$.

Theorem 4.2. *If p is an odd prime and $p|c$, then all powers of p are M-pseudoprimes.*

Proof. The characteristic polynomial of M is $\chi_M(x) = x^3 + bx + c$ and the eigenvalues $\lambda_1, \lambda_2, \lambda_3$ satisfy the following:

$$\begin{aligned} \lambda_1 + \lambda_2 + \lambda_3 &= 0 \\ \lambda_1\lambda_2 + \lambda_2\lambda_3 + \lambda_3\lambda_1 &= b \\ \lambda_1\lambda_2\lambda_3 &= -c \end{aligned}$$

The hypothesis says that $p|c$, so let $c = pk$ for $k \in \mathbb{Z}$. Then p^n, with $n \in \mathbb{N}$, is an M-pseudoprime if and only if:

$$\mathrm{Tr}(M^{p^n}) \equiv \mathrm{Tr}(M) \pmod{p^n}$$

In our case, this is equivalent to:

$${\lambda_1}^{p^n} + {\lambda_2}^{p^n} + {\lambda_3}^{p^n} \equiv 0 \pmod{p^n}.$$

We will prove this using induction. The base case for $n = 1$ is true by Fermat's Little Theorem for the prime p. Suppose the statement is true for n.

We have to show this implies that it is also true for $n+1$.

Let $u = {\lambda_1}^{p^n}, v = {\lambda_2}^{p^n}, w = {\lambda_3}^{p^n}$. Then, by our induction hypothesis, $u + v + w \equiv 0 \pmod{p^n}$, and we want to show that $u^p + v^p + w^p \equiv 0 \pmod{p^{n+1}}$. Note that $uvw = (\lambda_1\lambda_2\lambda_3)^{p^n} \equiv 0 \pmod{p^{n+1}}$.

Consider $S(i, p-i)$. Recall that:

$$S(i, p-i) = u^i v^{p-i} + u^i w^{p-i} + v^i u^{p-i} + v^i w^{p-i} + w^i u^{p-i} + w^i v^{p-i}$$

Each such S will be multiplied by a constant in the trinomial expansion of $(u+v+w)^p$. For any particular $\frac{p+1}{2} \leq i \leq p-1$, the coefficient is always divisible by p:

$$c_i = \binom{p}{i,\ p-i,\ 0} = \frac{p!}{i! \cdot (p-i)! \cdot 0!} = \frac{p!}{i! \cdot (p-i)!}$$

We then have that the trinomial expansion of $(u+v+w)^p$ can be conveniently written as:

$$(u+v+w)^p = u^p + v^p + w^p + \sum_{i=\frac{p+1}{2}}^{p-1} \Big(c_i \cdot S(i, p-i) \Big) + uvw \cdot \alpha$$

Here α is chosen such that it contains all the other terms of the trinomial expansion - uvw must divide this term. Using a technique similar to that used in Section 4.1, we can show that $uvw \cdot \alpha$ is divisible by p^{n+1}. Thus, it is sufficient to prove that

$$\sum_{i=\frac{p+1}{2}}^{p-1} c_i \cdot S(i, p-i)$$

is also divisible by p^{n+1}. Because every c_i is divisible by p, it is enough to prove that every $S(i, p-i)$ is a multiple of p^n.

We now can describe a key identity:

$$S(x, y) = (u+v+w) \cdot S(x-1, y) - S(x-1, y+1) - uvw \cdot S(x-2, y-1)$$

This is true for polynomials with integer coefficients. Reducing modulo p^n and using the induction hypothesis gives:

$$S(x, y) \equiv -S(x-1, y+1) \pmod{p^n}$$

Thus for all i:

$$S(i, p-i) \equiv -S(i-1, p-i+1) \equiv ... \equiv \pm S\left(\frac{p+1}{2}, \frac{p-1}{2}\right)$$

Now using the symmetry of S, consider $x = \frac{p+1}{2}$:

$$S\left(\frac{p-1}{2}, \frac{p+1}{2}\right) = S\left(\frac{p+1}{2}, \frac{p-1}{2}\right) \equiv -S\left(\frac{p-1}{2}, \frac{p+1}{2}\right)$$

But this means we have a number being equivalent to its negative in a modulus that is not divisble by 2. Thus we have that this number must be 0:

$$\sum_{i=\frac{p+1}{2}}^{p-1} c_i \cdot S(i, p-i) \equiv 0 \pmod{p^{n+1}}$$

This constitutes the last step in proving that $u^p + v^p + w^p \equiv 0 \pmod{p^{n+1}}$. As such the statement is true for $n+1$ and the induction argument is complete. Therefore, for p an odd prime that divides b, all powers of p are M-pseudoprimes.

□

We will now present another theorem for matrices with characteristic polynomial of the form

$$\chi_M(x) = x^3 + bx + c$$

Recall that we have:

$$\begin{aligned} \lambda_1 + \lambda_2 + \lambda_3 &= 0 \\ \lambda_1\lambda_2 + \lambda_2\lambda_3 + \lambda_3\lambda_1 &= b \\ \lambda_1\lambda_2\lambda_3 &= -c \end{aligned}$$

Theorem 4.3. *If p is a prime not equal to 3 and $p|b$, then all powers of p, p^n, are M-pseudoprimes.*

The idea of the proof is to induct on n. The inductive hypotheses will be:

1. $\lambda_1^{p^m} + \lambda_2^{p^m} + \lambda_3^{p^m} \equiv 0 \pmod{p^{m+1}}\ \forall\ m \leq n$
2. $(\lambda_1\lambda_2)^{p^m} + (\lambda_2\lambda_3)^{p^m} + (\lambda_3\lambda_1)^{p^m} \equiv 0 \pmod{p^{m+1}}\ \forall\ m \leq n$

We will first prove a lemma given these inductive hypotheses.

Lemma 4.4. *Given the above conditions, for all integers r such that r is not divisible by 3 and for any integer x such that $\frac{r}{2} \leq x \leq r$, we have $S(x, r-x) \equiv 0 \ (mod\, p^{n+1})$.*

Proof. By induction on r. We have the following identities:

$$\begin{aligned} S(x,y) &= (u+v+w)\cdot S(x-1,y) - S(x-1,y+1) \\ &\quad - uvw \cdot S(x-2,y-1) \\ &\equiv -S(x-1,y+1) - uvw \cdot S(x-2,y-1) \pmod{p^{n+1}} \end{aligned} \tag{1}$$

$$\begin{aligned} 2S(x+1,x) &= (u+v+w)\cdot S(x,x) - uvw \cdot S(x-1,x-1) \\ &\equiv -uvw \cdot S(x-1,x-1) \pmod{p^{n+1}} \end{aligned} \tag{2}$$

$$\begin{aligned} S(x) &= (u+v+w)\cdot S(x-1) - 2S(x-1,1) \\ &\equiv -2S(x-1,1) \pmod{p^{n+1}} \end{aligned} \tag{3}$$

$$\begin{aligned} S(x,x) &= (uv+vw+wu)\cdot S(x-1,x-1) - 2uvw \cdot S(x-1,x-2) \\ &\equiv -2uvw \cdot S(x-1,x-2) \pmod{p^{n+1}} \end{aligned} \tag{4}$$

We have 2 cases, determined by whether $r \equiv 1$ or $2 \pmod 3$. We thus have two base cases of $r = 1$ and $r = 2$:

Base Case 1.

$$S(1,0) = 2(u+v+w) \equiv 0 \ (mod\, p^{n+1})$$

Base Case 2.

$$\begin{aligned} S(1,1) &= 2(uv+vw+wu) \equiv 0 \ (mod\, p^{n+1}) \\ S(2,0) &= 2(u^2+v^2+w^2) \\ &= 2(u+v+w)^2 - 4(uv+vw+wu) \\ &\equiv 0 \ (mod\, p^{n+1}) \end{aligned}$$

So our base cases are done.

Inductive Assumption. *For all $k \in \mathbb{N}$ such that $k \leq r$ and $k \not\equiv 0 \ (mod\, 3)$, every $S(x, k-x) \equiv 0 \ (mod\, p^{n+1})$.*

Now consider each $S(x, r+3-x)$:

Case 1. $x = r+3$:

$$\begin{aligned} &S(x, r+3-x) = S(r+3, 0) = S(r+3) \\ &\equiv -2S(r+2, 1) \pmod{p^{n+1}} && \text{by (3)} \end{aligned}$$

Case 2. $x > r+4-x$:

$$\begin{aligned} &S(x, r+3-x) \equiv -S(x-1, r+4-x) \\ &\qquad\qquad - uvw \cdot S(x-2, r+2-x) && \text{by (1)} \\ &\equiv -S(x-1, r+4-x) \pmod{p^{n+1}} && \text{(inductive hypothesis)} \end{aligned}$$

Case 3. $x = r+4-x$:

$$\begin{aligned} &2S(x, r+3-x) = S(x, x-1) \\ &\equiv -uvw \cdot S(x-2, x-2) \pmod{p^{n+1}} && \text{by (2)} \\ &\equiv -uvw \cdot S(x-2, r+2-x) \pmod{p^{n+1}} \\ &\equiv 0 \pmod{p^{n+1}} && \text{(inductive hypothesis)} \end{aligned}$$

Case 4. $x = r+3-x$:

$$\begin{aligned} &S(x, r+3-x) = S(x, x) \\ &\equiv -2uvw \cdot S(x-1, x-2) \pmod{p^{n+1}} && \text{by (4)} \\ &\equiv 0 \pmod{p^{n+1}} && \text{(inductive hypothesis)} \end{aligned}$$

But now we can repeat the process described in Case 2:

$$\begin{aligned} S(x, r+3-x) &\equiv -S(x-1, r+4-x) \\ &\equiv S(x-2, r+5-x) \\ &\vdots \\ &\equiv \pm S(\alpha, \beta) \end{aligned}$$

Here we keep repeating the process until we get $0 \le \alpha - \beta \le 1$. Then if $\alpha = \beta + 1$:

$$\begin{aligned} S(x, r+3-x) &\equiv -S(x-1, r+4-x) \\ &\equiv S(x-2, r+5-x) \\ &\vdots \\ &\equiv \pm S\left(\frac{r+4}{2}, \frac{r+2}{2}\right) \\ &\equiv 0 \pmod{p^{n+1}} && \text{by case 3 above} \end{aligned}$$

If instead $\alpha = \beta$:

$$S(x, r+3-x) \equiv -S(x-1, r+4-x)$$

$$
\begin{aligned}
&\equiv S(x-2, r+5-x) \\
&\equiv -S(x-3, r+6-x) \\
&\vdots \\
&\equiv \pm S\left(\frac{r+3}{2}, \frac{r+3}{2}\right) \\
&\equiv 0 \pmod{p^{n+1}} \qquad \text{by case 4 above}
\end{aligned}
$$

We can repeat this process once with base case when $r \equiv 1 \pmod 3$ and once with base case when $r \equiv 2 \pmod 3$. Thus we have proved that, given the Inductive Assumption, regardless of the starting value of x, each $S(x, r+3-x) \equiv 0 \pmod{p^{n+1}}$. Our base case is already done, so by the principle of mathematical induction we have proved Lemma 4.4. □

We can now prove Theorem 4.3.

Proof. We prove Theorem 4.3 by induction on n. Recall that we have our inductive hypotheses as well as Lemma 4.4:

1. $\lambda_1^{p^m} + \lambda_2^{p^m} + \lambda_3^{p^m} \equiv 0 \pmod{p^{m+1}} \; \forall \; m \leq n$
2. $(\lambda_1\lambda_2)^{p^m} + (\lambda_2\lambda_3)^{p^m} + (\lambda_3\lambda_1)^{p^m} \equiv 0 \pmod{p^{m+1}} \; \forall \; m \leq n$
3. $\forall \; x, y \in \mathbb{N}$ such that $x + y \not\equiv 0 \pmod 3$, $S(x, y) \equiv 0 \pmod{p^{n+1}}$

Again, let $u = {\lambda_1}^{p^n}, v = {\lambda_2}^{p^n}, w = {\lambda_3}^{p^n}$. Our base case is when $n = 0$. Now $\lambda_1^{p^0} + \lambda_2^{p^0} + \lambda_3^{p^0} = \lambda_1 + \lambda_2 + \lambda_3 = 0$ and $p^1|0$. Similarly, $(\lambda_1\lambda_2)^{p^0} + (\lambda_2\lambda_3)^{p^0} + (\lambda_3\lambda_1)^{p^0} = \lambda_1\lambda_2 + \lambda_2\lambda_3 + \lambda_3\lambda_1 = b$, and $p|b$ so $p^1|b$. So our base case is done.

Now consider $(u + v + w)^p$:

$$
= u^p + v^p + w^p + \sum_{j=1}^{\lfloor \frac{p}{3} \rfloor} \left((uvw)^j \cdot \sum_{i=\lceil \frac{p+3j}{2} \rceil}^{p-3j} (S(i, p-3j-i) \cdot c_x) \right)
$$

Here each c_x is a trinomial coefficient and in particular is divisible by p:

$$
c_x = \binom{p}{i+j, \; p-2j-i, \; j}
$$

Note $p \neq 3$ implies that Lemma 4.4 applies to each $S(i, p-3j-i)$. Thus each term within the inner summation is divisible by $p^{n+1} \cdot p = p^{n+2}$.

Further note that since $u+v+w \equiv 0 \pmod{p^{n+1}}$, we have $(u+v+w)^p \equiv 0 \pmod{p^{n+2}}$. We can thus reduce the summation modulo p^{n+2} to get:

$$u^p + v^p + w^p = \lambda_1^{p^{n+1}} + \lambda_2^{p^{n+1}} + \lambda_3^{p^{n+1}} \equiv 0 \pmod{p^{n+2}}$$

This was the first part of the inductive hypothesis for $n+1$. Now consider the term $(uv+vw+wu)^p$:

$$= (uv)^p + (vw)^p + (wu)^p + \sum_{j=1}^{\lfloor \frac{p}{3} \rfloor} \left((uvw)^j \cdot \sum_{i=\lceil \frac{2p-3j}{2} \rceil}^{\min(2p-3j,\, p-j)} (S(i, p-3j-i) \cdot c_x) \right)$$

Here each c_x is defined as in the first summation, via trinomial coefficients:

$$c_x = \binom{p}{i+j,\ p-2j-i,\ j}$$

The same analysis as for the first summation gives us:

$$0 \equiv (uv+vw+wu)^p \equiv (uv)^p + (vw)^p + (wu)^p \pmod{p^{n+2}}$$

And so the other condition we inducted on has now also been proved for the next term up. Since the base case has been discussed previously, by the principle of mathematical induction we are done.

□

4.3 3×3 matrices with trace ±1

We now consider matrices with the characteristic polynomial of the form

$$\chi_M(x) = x^3 \pm x^2 + bx + c$$

Note that when the characteristic polynomial is $\chi_M(x) = x^3 - x^2 + bx + c$, we have $\mathrm{Tr}(M) = 1$. When the polynomial is $\chi_M(x) = x^3 + x^2 + bx + c$, we have $\mathrm{Tr}(M) = -1$.

Theorem 4.5. *For a matrix M with integer entries and with characteristic polynomial $\chi_M(x) = x^3 \pm x^2 + bx + c$, if p is an odd prime that divides both b and c, then all powers of p are M-pseudoprimes.*

Remark: If the trace is 1, then $p = 2$ and its powers also work.

Proof. We will induct on powers n of the matrix. This proof is quite similar to that of Theorem 4.3, so some details are omitted. As b and c are even, we write them as $b = pd$ and $c = pe$, for d, e are integers. We know:

$$\begin{aligned}\lambda_1 + \lambda_2 + \lambda_3 &= \mathrm{Tr}(M) = \pm 1\\ \lambda_1\lambda_2 + \lambda_2\lambda_3 + \lambda_3\lambda_1 &= pd\\ \lambda_1\lambda_2\lambda_3 &= -pe\end{aligned}$$

The induction hypothesis is:

1. $\lambda_1^{p^n} + \lambda_2^{p^n} + \lambda_3^{p^n} \equiv 0 \pmod{p^n}$, i.e. the condition for p^n to be a pseudoprime
2. $(\lambda_1\lambda_2)^{p^n} + (\lambda_2\lambda_3)^{p^n} + (\lambda_3\lambda_1)^{p^n} \equiv 0 \pmod{p^n}$

The base case, $n = 0$, is true by Fermat's Little Theorem on integers. Suppose the induction hypothesis holds for n; we will show that it is also true for $n + 1$, thus making p^{n+1} a pseudoprime.

Let $u = \lambda_1^{p^n}, v = \lambda_2^{p^n}, w = \lambda_3^{p^n}$. Thus, proving that p^{n+1} is a pseudoprime means proving that

$$u^p + v^p + w^p \equiv \mathrm{Tr}(M) \pmod{p^{n+1}}$$

Let us define S as in the previous section:

$$S(x, y, z) = u^x v^y w^z + u^x w^y v^z + v^x u^y w^z + v^x w^y u^z + w^x u^y v^z + w^x v^y u^z$$

Let us look at the expansion $(u + v + w)^p$:

$$(u + v + w)^p =$$

$$u^p + v^p + w^p + \sum_{i=\frac{p+1}{2}}^{p-1} \binom{p}{i} S(i, p-i, 0) + \sum_{i \geq j \geq p-i-j > 0} \binom{p}{i, j, p-i-j} S(i, j, p-i-j)$$

We know that $(u+v+w)^p$ is congruent to $\mathrm{Tr}(M)$ modulo p^{n+1} since $1^{p^n} \equiv 1 \pmod{p^{n+1}}$ and $(-1)^{p^n} \equiv -1 \pmod{p^{n+1}}$, for odd primes p. So we have:

$$\begin{aligned}\mathrm{Tr}(M) \equiv \mathrm{Tr}(M^{p^{n+1}}) &+ \sum_{i=\frac{p+1}{2}}^{p-1} \binom{p}{i} S(i, p-i, 0)\\ &+ \sum_{i \geq j \geq p-i-j > 0} \binom{p}{i, j, p-i-j} S(i, j, p-i-j) \pmod{p^{n+1}}\end{aligned}$$

We want to show that both sums are divisible by p^{n+1}.

The first sum has the binomial coefficients divisible by p, so it is enough to show that every $S(i, p-i, 0)$ is divisible by p^n. We already know that each such S is an integer, because of the Fundamental Theorem of Symmetric Polynomials.

As we did in Theorem 4.3, we find a recurrence for $S(i, p-i, 0)$:

$$S(i, p-i, 0) =$$

$$(u+v+w)S(i-1, p-i-1, 0) - S(i-1, p-i, 1) - S(i, p-i-1, 1)$$

From the induction hypothesis, $uv + vw + wu \equiv 0 \pmod{p^n}$, so $(uv + vw + wu)S(i-1, p-i-1, 0)$ is divisible by p^n.

Because each $S(i-1, p-i, 1)$ and $S(i, p-i-1, 1)$ is divisible by $uvw = \lambda_1^{p^n}\lambda_2^{p^n}\lambda_3^{p^n} = p^{p^n}(-e)^{p^n}$, each of them must be divisible by p^n. Hence we can state that:

$$\sum_{i=\frac{p+1}{2}}^{p-1} \binom{p}{i} S(i, p-i, 0) \equiv 0 \pmod{p^{n+1}}$$

Each S in the second sum is divisible by $uvw = \lambda_1^{p^n}\lambda_2^{p^n}\lambda_3^{p^n} = p^{p^n}(-e)^{p^n}$. This, alongside the Fundamental Theorem of Symmetric Polynomials, means that we can state:

$$\sum_{i \geq j \geq p-i-j > 0} \binom{p}{i, j, p-i-j} S(i, j, p-i-j) \equiv 0 \pmod{p^{n+1}}$$

Thus we have proved the first part of the inductive step. The second part follows similarly, since proving that $(uv)^{p^{n+1}} + (vw)^{p^{n+1}} + (wu)^{p^{n+1}} \equiv 0 \pmod{p^{n+1}}$ comes from a similar summation where every term is divisible by uvw. From all of the above, we have just proved that

$$\mathrm{Tr}\left(M^{p^{n+1}}\right) \equiv \mathrm{Tr}(M) \pmod{p^{n+1}},$$

so p^{n+1} is an M-pseudoprime. The remark regarding powers of 2 can be proved by noticing that 1 raised to any power will still be 1, so $(u+v+w)^{p^n} \equiv u+v+w \pmod{p^{n+1}}$ regardless of the parity of p. $\square$

4.4 Prime factorizations of pseudoprimes

Of particular interest to us was the **Königsberg matrix** and its associated pseudoprimes. Based on the famous *Seven Bridges of Königsberg problem*, concerning walks on a graph representing bridges in the then-Prussian city of Königsberg, the Königsberg matrix is simply the adjacency matrix of said graph. The matrix and its associated characteristic polynomial are:

$$K = \begin{pmatrix} 0 & 2 & 1 & 0 \\ 2 & 0 & 1 & 2 \\ 1 & 1 & 0 & 1 \\ 0 & 2 & 1 & 0 \end{pmatrix}, \ \chi(x) = x^4 - 11x^2 - 8x$$

Indeed, the characteristic polynomial fully encodes the information we need for the pseudoprimes since we can work out the trace of successive powers of the matrix via the coefficients of the polynomial (as described in section 2.2).

In this particular case, we can further reduce the polynomial to the case of $x^3 - 11x - 8$ since an eigenvalue of 0 adds nothing to the trace of the powers of the matrix. We can then apply Theorem 4.3 to this polynomial to conclude that all powers of 11 are Königsberg pseudoprimes. We can do better, and generalize to any suitable matrix. First we prove a lemma.

Lemma 4.6. *For any prime p such that p is not 2 or 3, there are infinitely many primes $q \neq p$ such that $q \not\equiv -1 \pmod{p}$ and $q^3 \not\equiv 1 \pmod{p}$.*

Proof. We have up to 5 distinct conditions on q modulo p. Two come from the fact that $q \neq 0, -1$ modulo p, and up to three come from the 3 possible distinct cube roots of unity (modulo p). If $p > 5$, then there are more than 5 distinct residues modulo p and so we can simply choose the remainder that isn't explicitly prohibited; this cannot be 0. Thus, we can then apply Dirichlet's Theorem on Arithmetic Progressions to find infinitely many q such that the required conditions are satisfied.

If instead $p = 5$, notice that $2 \neq -1 \pmod 5$ and $2^3 = 3 \neq 1$, so we can apply Dirichlet's Theorem on Arithmetic Progressions to find infinitely many primes that are 2 modulo 5. Thus we have proved the lemma. □

Theorem 4.7. *Given a particular characteristic polynomial $x^3 + bx + c$, suppose a prime p satisfies the following conditions:*

- *$p \neq 2, 3$*
- *p satisfies either of the conditions in Theorem 4.2 or Theorem 4.3*

Then there are infinitely many primes $q \neq p$ such that $q \cdot p^n$ is a pseudoprime for infinitely many $n \in \mathbb{N}$.

Proof. Recall that we want

$$K(q \cdot p^n) = \lambda_1^{q \cdot p^n} + \lambda_2^{q \cdot p^n} + \lambda_3^{q \cdot p^n} \equiv 0 \pmod{q \cdot p^n}$$

We will construct q such that divisibility by q is guaranteed, and we will show that divisibility by p^n comes as a direct consequence of Theorems 4.2 and 4.3.

Take q such that $q \not\equiv -1 \pmod{p}$ and $q^3 \not\equiv 1 \pmod{p}$. Note that Lemma 4.6 gives us that there are infinitely many primes that satisfy these congruences. Consider the sequence $K(i)$ modulo our prime q as i varies through naturals. There are a finite number of residues modulo q. Since each $K(i)$ is determined exactly by the previous three terms, a pigeonhole argument implies that our sequence $K(i)$ must be periodic. By results of Galois Theory, we know that this period divides the LCM of $q-1$, q^2-1 and q^3-1. Thus let X be an integer such that:

$$X = (q+1)(q^3-1)$$

The construction of q gives that $p \nmid X$, and so $\text{GCD}(X, p) = 1$. This means the order of p modulo X exists; let it be N, so that $p^N \equiv 1 \pmod{X}$

Now we consider $K(q \cdot p^N) \pmod{q}$. We know that, modulo q, $K(i)$ has period X as i varies through naturals, so we can take the input to the function modulo X without changing the output:

$$\begin{aligned} & K(q \cdot p^N) \pmod{q} \\ \equiv\ & K(q \cdot p^N \pmod{X}) \pmod{q} \\ \equiv\ & K(q) \pmod{q} \end{aligned}$$

But now we can apply Fermat's Little Theorem for matrices on the last equivalence relation to get:

$$\begin{aligned} & K(q \cdot p^N) \pmod{q} \\ \equiv\ & K(q) \pmod{q} \\ \equiv\ & K(1) \pmod{q} \\ \equiv\ & 0 \pmod{q} \end{aligned}$$

Thus divisibility by q is guaranteed. Now similar arguments used to those in the proofs of Theorems 4.2 and 4.3 can be used, recalling that the base

case is always satisfied since $\lambda_1 + \lambda_2 + \lambda_3 = 0$ and we only require divisibility conditions during our inductive proof. This gives divisibility by p^N, thus proving that $q \cdot p^N$ is a pseudoprime. We can set $n = N + kX$ for any integer k to obtain infinitely many n, thus proving Theorem 4.7.

□

With regards to the Königsberg matrix, we have now proved that as long as 11 does not divide the value $(q+1)(q^3-1)$ for a fixed prime $q \neq 2, 3$, q will appear infinitely many times in the list of Königsberg pseudoprimes.

4.5 $n \times n$ matrices with trace 0

Inspired by the results of 3×3 matrices, we give a more general result. We will first need the following lemma:

Lemma 4.8. *Consider a symmetric polynomial of odd degree in n variables $P(x_1, x_2, \cdots, x_n)$. Let Q be the unique polynomial in the n-variable polynomial ring $A[\sigma_1, \sigma_2, ..., \sigma_n]$ that defines P. Then each monomial of Q contains a σ_i with i odd.*

Proof. Note that the degree of P is odd, so we must have that each term of Q is also odd. But since even symmetrical polynomials $(\sigma_2, \sigma_4, \cdots)$ can only multiply to give polynomials of even degree, each term must therefore have an odd degree elementary symmetrical polynomial. □

We can now state our main result:

Theorem 4.9. *For a matrix that has characteristic polynomial of form $x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n$ with $a_1 = 0$, let p be a prime such that $p \neq 2$ and p divides each a_i for all odd i. Then all powers of p are pseudoprimes.*

Proof Sketch. We proceed by induction on r. Let $u_1 = \lambda_1^{p^r}, u_2 = \lambda_2^{p^r}, \cdots, u_n = \lambda_n^{p^r}$. Consider elementary polynomials in the n variables $u_1, \cdots, u_n$.

Inductive Assumption. *Let each σ_i be an elementary symmetric polynomial on the indeterminates $u_1, \cdots, u_n$. Then if i is odd, σ_i is divisible by p^r.*

We will show how, given the inductive hypothesis, $\rho(\sigma_1)$ and $\rho(\sigma_3)$ will both be divisible by p^{r+1}, as required. The general $\rho(\sigma_i)$ case follows similarly.

Note that the base case follows from Vieta's formulas and the hypotheses of the theorem. We can write $\sum_{i=1}^{n} ({u_i}^p) = \rho(\sigma_1, p)$ in terms of these $\sigma_1, \cdots, \sigma_n$:

$$\sum_{i=1}^{n} {u_i}^p = \rho(\sigma_1, p) = \sigma_1^p + Q'(\sigma_1, \cdots, \sigma_n)$$

Here Q' is a symmetric polynomial in the polynomial ring. All coefficients of Q' are divisible by p as they come from a multinomial expansion. We can then use Lemma 4.8 to conclude that every monomial in Q' must be divisible by some σ_i with odd i. But now our inductive hypothesis gives us that $\sigma_i \equiv 0 \pmod{p^n}$, so we get that $Q' \equiv 0 \pmod{p^{n+1}}$.

Since σ_1^p is divisible by p^{n+1}, we get that $\rho(\sigma_1, p) \equiv 0 \pmod{p^{n+1}}$, as is required by the induction. But this is only the first part of our inductive step; we now need to show that each $\rho(\sigma_i, p) \equiv 0 \pmod{p^{n+1}}$ for odd i. Consider $\rho(\sigma_3, p)$:

$$\rho(\sigma_3, p) = (u_1u_2u_3)^p + (u_1u_2u_4)^p + \cdots + (u_{n-2}u_{n-1}u_n)^p$$

We let $v_1 = u_1u_2u_3,\ v_2 = u_1u_2u_4,\ \cdots,\ v_{\binom{n}{3}} = u_{n-2}u_{n-1}u_n$. Now consider the elementary symmetric polynomials of form $\sigma'_j[v_1, \cdots, v_{\binom{n}{3}}]$. We want to prove that $\sigma'_1 \equiv 0 \pmod{p^{n+1}}$. But we can use exactly the same proof as that used for σ_1, by noting that each σ'_j can be written as a linear combination of various σ_i where i is odd.

This technique generalizes - each $\rho(\sigma_i, p)$ (with odd i) can be written as a linear combination of σ_j (with j odd), and thus we have proved that each $\rho(\sigma_i, p) \equiv 0 \pmod{p^{n+1}}$.

The principle of mathematical induction means that we are done, and thus all powers of p are indeed pseudoprimes for the matrix.

□

4.6 Pseudoprimes of block diagonal matrices

Given an $n \times n$ matrix M and its pseudoprimes, let us consider N, the block diagonal matrix formed by using k blocks of M.

$$N = \begin{pmatrix} M & 0 & \dots & 0 \\ 0 & M & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & M \end{pmatrix}$$

From Section 2.2, the following statements are true:

$$\begin{aligned} \mathrm{Tr}(N) &= k \cdot \mathrm{Tr}(M) \\ (\forall p \in \mathbb{N})\ \mathrm{Tr}(N^p) &= k \cdot \mathrm{Tr}(M^p) \end{aligned}$$

Theorem 4.10. *All pseudoprimes r of the matrix M are pseudoprimes of the matrix N (with M and N being defined as above).*

Proof. Let r be a pseudoprime of M. From FℓT we know that $\mathrm{Tr}(M^r) \equiv \mathrm{Tr}(M) \pmod{r}$. This implies that for any natural k we have:

$$k \cdot \mathrm{Tr}(M^r) \equiv k \cdot \mathrm{Tr}(M) \pmod{r} \iff \mathrm{Tr}(N^r) \equiv \mathrm{Tr}(N) \pmod{r}$$

This means that r is in fact a pseudoprime for any block diagonal matrix N formed from M-blocks. □

4.7 Extending Carmichael numbers: PROMYS Pseudoprimes

We previously introduced the Carmichael numbers, which are in a sense 'immune' to Fermat's Little Theorem, since they pass Fermat's primality test for each integer a. Our motivating question is whether these Carmichael-esque numbers exist for n by n matrices. We will present two useful lemmas before tackling 'PROMYS pseudoprimes'.

Lemma 4.11. $K(1) \equiv K(p) \equiv K(p^n) \pmod{p}$

Proof. The first equivalence is simply FℓT for matrices. The second equivalence is realised by induction and considering the multinomial expansion of $(\lambda_1 + \cdots + \lambda_n)^p$. □

Lemma 4.12. *There are no pseudoprimes that are immune to every matrix i.e. that pass the primality test for every matrix.*

Proof. Consider any number $n \neq 1$. n has a prime divisor, so let $n = pb$, with p prime. Let M be a p by p matrix whose characteristic polynomial has coefficients $[1, 1, 1, 1, ...]$. By considering the traces of the powers of M, we see that we get this sequence:

$$(-1, -1, \cdots, p-1, -1, -1, \cdots, p-1, -1, -1, \cdots)$$

This sequence repeats with period p. This means that $K(px)$ will have value $p - 1$ for all naturals x.

Now note that $p - 1 \equiv -1 \pmod{px}$ implies that $p \equiv 0 \pmod{px}$ which in turn implies that $px|p$. But this is only true when $x = 1$ i.e. when p itself is prime. Thus all px that are multiples of p with x not equal to 1 cannot possibly be congruent to -1 (mod px) and so cannot be pseudoprimes with respect to the matrix M. □

Having ruled out the possibility of these 'super-immune' pseudoprimes, we now define what we call a 'PROMYS pseudoprime'.

Definition. *A PROMYS pseudoprime is some natural number n where n is not prime and for every 2×2 matrix M, n passes its Fermat primality test.*

Inspired by Korselt's Criterion, we now present a sufficient condition for n to be a PROMYS Pseudoprime:

Theorem 4.13. *$n \in \mathbb{N}$ is a PROMYS pseudoprime if the following conditions are satisfied:*

1. *n is not prime*
2. *n is square-free*
3. *For all $p|n$, p prime, $n \equiv 1 \ (mod\, p - 1)$*
4. *$n \equiv 1$ or $n \equiv p \ (mod\, p^2 - 1)$*

Proof. We will prove that $K(n) \equiv K(1) \bmod p$ for each p dividing n. Consider the sequence $(K(1), K(2), \cdots)$. The argument in Theorem 4.7 gives us that this sequence has a period that divides either $p - 1$ or $p^2 - 1$. Thus we know that for all integers r:

$$K(1 + r(p-1)) \equiv K(1) \pmod{p}$$
$$\text{or}$$
$$K(1 + r(p^2-1)) \equiv K(1) \pmod{p}$$

By construction we have that $n \equiv 1 \pmod{p-1}$. So if the first case is true, we have that $K(n) \equiv K(1) \pmod{p}$, as required. If the second case is true, then we can use Lemma 4.11 to show that $n \equiv 1 \pmod{p^2-1}$ or $n \equiv p \pmod{p^2-1}$ is sufficient for $K(n) \equiv K(1)$.

Thus we have that for each prime p dividing n, $K(n) \equiv K(1) \pmod{p}$. Since n is square-free by construction, we can combine all of the congruences via Chinese Remainder Theorem and get that $K(n) \equiv K(1) \pmod{n}$. Since

n is not prime by construction, we have that n is a pseudoprime for every 2×2 matrix, i.e. it is a PROMYS pseudoprime.

□

We now extend this idea further:

Definition. *A k-PROMYS pseudoprime is some natural number n where n is not prime and for every $k \times k$ matrix M, n passes its Fermat primality test.*

Note that by this definition 1-PROMYS pseudoprimes are just the Carmichael numbers. We now present the following theorem:

Theorem 4.14. *The following conditions are sufficient for n to be a k-PROMYS pseudoprime:*

1. *n is not prime*
2. *n is square-free*
3. *For all integers j such that $1 \leq j \leq k$, and for all primes p dividing n, $n \equiv p^i \ (mod\, p^j - 1)$ for some intger i.*

Proof Sketch. The proof follows via precisely the same arguments used in Theorem 4.13. We analyze the residue of n modulo each prime p dividing n, and conclude, via Lemma 4.11, that it is indeed the same as $K(1)$. We then use Chinese Remainder Theorem to conclude that $K(n) \equiv K(1) \pmod{n}$, so n must be a k-PROMYS pseudoprime.

□

Are there any k-PROMYS pseudoprimes for $k \geq 2$? By checking all the Carmichael numbers up to 10^{17}, we were able to find two 2-PROMYS pseudoprimes:

$$\begin{aligned}
443372888629441 &= 17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331 \\
&\equiv 1 \pmod{16,\ 30,\ 40,\ 42,\ 88,\ 96,\ 166,\ 330} \\
&\equiv 1 \pmod{17^2 - 1,\ 31^2 - 1,\ 41^2 - 1,\ 43^2 - 1,\ 89^2 - 1,} \\
&\qquad\qquad 97^2 - 1,\ 167^2 - 1,\ 331^2 - 1) \\
39671149333495681 &= 17 \cdot 37 \cdot 41 \cdot 71 \cdot 79 \cdot 97 \cdot 113 \cdot 131 \cdot 191 \\
&\equiv 1 \pmod{16,\ 36,\ 40,\ 70,\ 78,\ 96,\ 112,\ 130,\ 190} \\
&\equiv 1 \pmod{17^2 - 1,\ 37^2 - 1,\ 41^2 - 1,\ 71^2 - 1,\ 79^2 - 1,} \\
&\qquad\qquad 97^2 - 1,\ 113^2 - 1,\ 131^2 - 1,\ 191^2 - 1)
\end{aligned}$$

Neither of these are 3-PROMYS pseudoprimes, but see Section 5.3 for our unproved conjectures regarding k-PROMYS pseudoprimes in general.

5 Numerical data analysis

Finally, we will lay out some other observations we gathered from numerical data, but have not proven. Our data was collected via Python code we wrote, which can be viewed at: https://github.com/PinkPandaPresident/Pseudoprimes.

5.1 Interesting observations

Observation 1. Carmichael numbers such as 561 and 1105 often appear as matrix pseudoprimes. The number 1105 appears as a pseudoprime in approximately one fourth to one third of all the matrices we tested.

The next few observations listed are based on the investigation of matrices with characteristic polynomial $x^3 + bx + c$.

Observation 2. When $b = 3$ and $c = \pm 2^n$ for natural n, 6 is always a pseudoprime. (Checked up to $n = 10$.)

Observation 3. When $b = -3$ and $c = \pm 2$ for natural n, all pseudoprimes p satisfy $2^p \equiv \pm 2 \pmod{p}$. (Checked for pseudoprimes up to 10000.)

Observation 4. When $b = 0$ and $c = \pm 2^n$ for natural n, for all n, the same set of pseudoprimes is generated. (Checked up to $n = 10$).

Observation 5. When $b = 3^n$ for natural n and $c = 0$, for all n, the same set of pseudoprimes are generated. (Checked for up to $n = 10$).

5.2 Frequency of pseudoprimes

Figure 1 shows the frequency of Königsberg pseudoprimes and Carmichael numbers up to a certain $n \in \mathbb{Z}$. A logarithmic scale is used on both axes to make the data more readable. As shown on the graph, the trend for both Königsberg pseudoprimes and for Carmichael numbers becomes approximately linear as n becomes large enough. In addition, while the density of Königsberg pseudoprimes is higher to begin with, for large enough values, namely when $n > 10^6$, the density of Königsberg pseudoprimes is less than that of the Carmichael numbers. Therefore, we can say that, for numbers larger than 10^6, using the Königsberg primality test is more effective than using any base-n primality test since it yields fewer pseudoprimes.

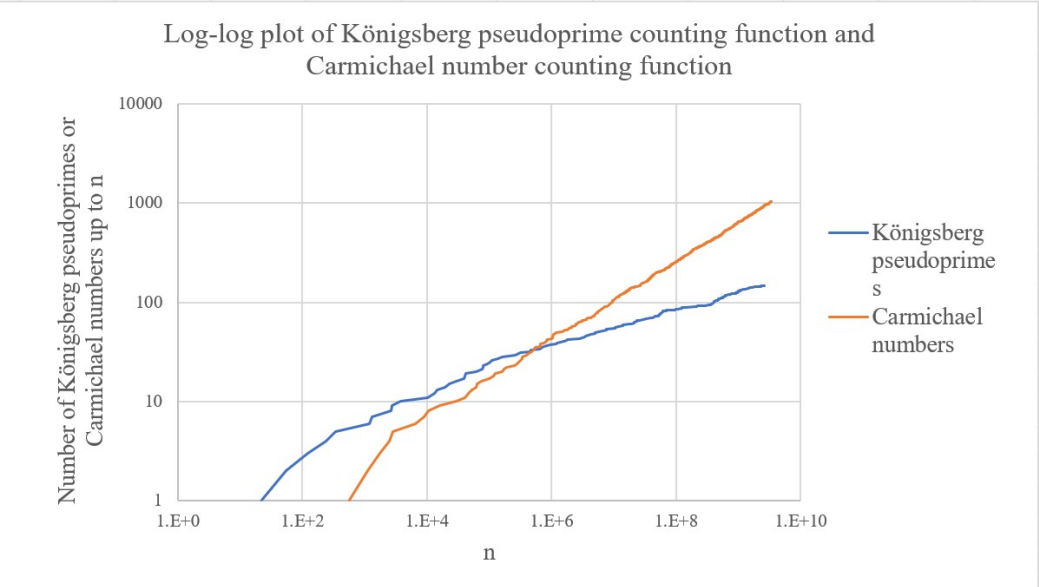

Figure 1: *The frequency of Königsberg pseudoprimes compared to the frequency of Carmichael numbers*

5.3 Conjectures

Conjecture 5.1. *All matrices generate infinitely many pseudoprimes.*

We have proved that this conjecture holds for many families of matrices, as detailed in Section 4; we believe it is true in general.

Conjecture 5.2. *Every prime p has some multiple that is a pseudoprime with respect to an arbitrary matrix M, as long as multiples of p are not explicitly ruled out by congruence analysis.*

This is a strong conjecture, and unproved for almost all matrices. In the case of the Königsberg matrix, for example, the first multiple of 3 that is a pseudoprime is $365191905 = 3 \cdot 5 \cdot 13 \cdot 43 \cdot 97 \cdot 449$. Some progress on this conjecture has been made in Section 4.4.

Conjecture 5.3. *There are infinitely many k-PROMYS pseudoprimes.*

This conjecture holds for $k = 1$ as it is known that there are infinitely many Carmichael numbers. Note this conjecture also directly implies Conejecture 5.1. More details are given in Section 4.7.

Conjecture 5.4. *The conditions given in Theorem 4.14 are necessary and sufficient for n being a k-PROMYS pseudoprime.*

We have already proved the sufficient part of this conjecture in the proof for Theorem 4.14; we conjecture that these conditions are necessary as well. Note that this conjecture has been proved for Carmichael numbers, the 1-PROMYS pseudoprimes.

Conjecture 5.5. *The pseudoprime-counting function $F_M(x)$ with respect to a matrix M is asymptotic to a function $f(x) = \alpha x^\beta$, where α and β are fixed constants that depend on M.*

This conjecture arises from the numerical data we have collected.

For matrices with characteristic polynomials in the form $x^3 + ax^2 + bx + c$, where $a \neq 0$, we conjecture that the following are true, based on numerical data obtained by testing all combinations of $-10 \leq a,\ b,\ c \leq 10,\ a \neq 0$:

Conjecture 5.6. *When $a = -1$, the powers of all prime factors of $b + c$ are pseudoprimes. Exception: When b, c are both odd, powers of 2 are not pseudoprimes.*

Conjecture 5.7. *When $a = 1$, the powers of all prime factors of $b - c$ are pseudoprimes. Exception: powers of 2 never appear.*

Conjecture 5.8. *When $a = -2$, for each prime factor p of $a + b + 1$, when $c \equiv 0 \ (mod\, p)$, all powers of p are pseudoprimes. Also, if :*

- *$|a + b| = q$, for a prime q*
- *$c \equiv -1 \ (mod\, q)$*

Then we have that all powers of q are pseudoprimes. Exception: If $a+b+1 = 1$, then all powers of the prime factors of $c+1$ are pseudoprimes (but powers of 2 and 3 never appear when $a + b + 1 = 1$).

Conjecture 5.9. *When $a = 2$, for each prime factor p of $a - b - 1$, when $c \equiv 0 \ (mod\, p)$, all powers of p are pseudoprimes. Also, if:*

- *$|a - b| = q$ for a prime q*
- *$c \equiv 1 \ (mod\, q)$*

Then we have that all powers of q are pseudoprimes. Exception: If $a-b-1 = -1$, then all powers of the prime factors of $c-1$ are pseudoprimes (but powers of 3 never appear when $a + b + 1 = 1$). Powers of 2 never appear.

Conjecture 5.10. *When $a = -3$, for each prime factor p of $a+b$, when $c \equiv -1 \ (mod\, p)$, all powers of p are pseudoprimes. If $a + b = 0$, all powers of prime factors of $c + 1$ are pseudoprimes.*

a	b	c	Powers
-1	2	3	5
-1	3	-9	3
1	2	5	3
1	2	-2	none
-2	-5	6	2, 7
-2	2	4	5
2	1	-10	5
2	1	6	3
-3	5	-3	2
-3	2	-2	none
3	-6	4	3
3	4	-2	none

Table 1: *Numerical examples regarding matrices with characteristic polynomial* $x^3 + ax^2 + bx + c$

Conjecture 5.11. *When* $a = 3$*, for each prime factor* p *of a-b, when* $c \equiv 1 \pmod{p}$*, all powers of* p *are pseudoprimes. Exception: Powers of 2 never appear.*

In general, the rules for $a = -x$, including the exceptions, can be transformed into those for $a = x$ by switching all $+$ to $-$ and vice versa. The only additional exception is that when $a > 0$, powers of 2 never appear.

Table 1 presents a few examples for the conjectures regarding powers of primes amongst the pseudoprimes generated by matrices with characteristic polynomial $x^3 + ax^2 + bx + c$, where $a \neq 0$. It includes both general cases and exceptions. The powers displayed are results obtained from testing primes up to 47.

6 Conclusion

In this paper, we first introduced an extension of Fermat's Little Theorem to matrices, and show how, like the original FℓT, a primality test can be devised around this theorem. We presented two proofs of this theorem in Section 3. We then investigated the scenarios in which this test fails - the false positives of the test, i.e. the pseudoprimes. In particular, we focused on matrices that have a trace equal to 0.

We showed that for a large class of 2×2 and 3×3 matrices, infinite families of pseudoprimes exist, defined by a prime and all of its powers (Theorems 4.2 and 4.3). Additionally, we showed that multiplying suitably large powers of this prime by a single other prime leads to another infinite family of pseudoprimes (Theorem 4.7). We then extended this theorem to show that an n by n zero-trace matrix represented by a characteristic polynomial with suitably divisible coefficients will also share these properties (Theorem 4.9).

We proceeded to analyze particular examples of matrices with trace of one, in particular proving that powers of primes were often pseudoprimes (Section 4.3). We looked at the Königsberg matrix, and block diagonal matrices (Sections 4.3, 4.4). We also defined 'k-PROMYS pseudoprimes', found two 2-PROMYS pseudoprimes, and gave sufficient conditions to find such pseudoprimes in general (Section 4.7).

We finished by stating our unproved conjectures, primarily concerning matrices with trace not zero and the infinitude of pseudoprimes for all matrices. We finally presented some of the numerical data we have gathered.

7 Acknowledgements

We would like to thank David Lowry-Duda for proposing such an intriguing project. We would also like to express our gratitude to Dragoș Crișan and George Robinson, for their guidance throughout this mathematical experience. Finally, we would like to thank the Clay Mathematics Institute, the Oxford Mathematical Institute, and everyone who had a hand in making PROMYS Europe happen and creating an engaging mathematical environment for all of us.